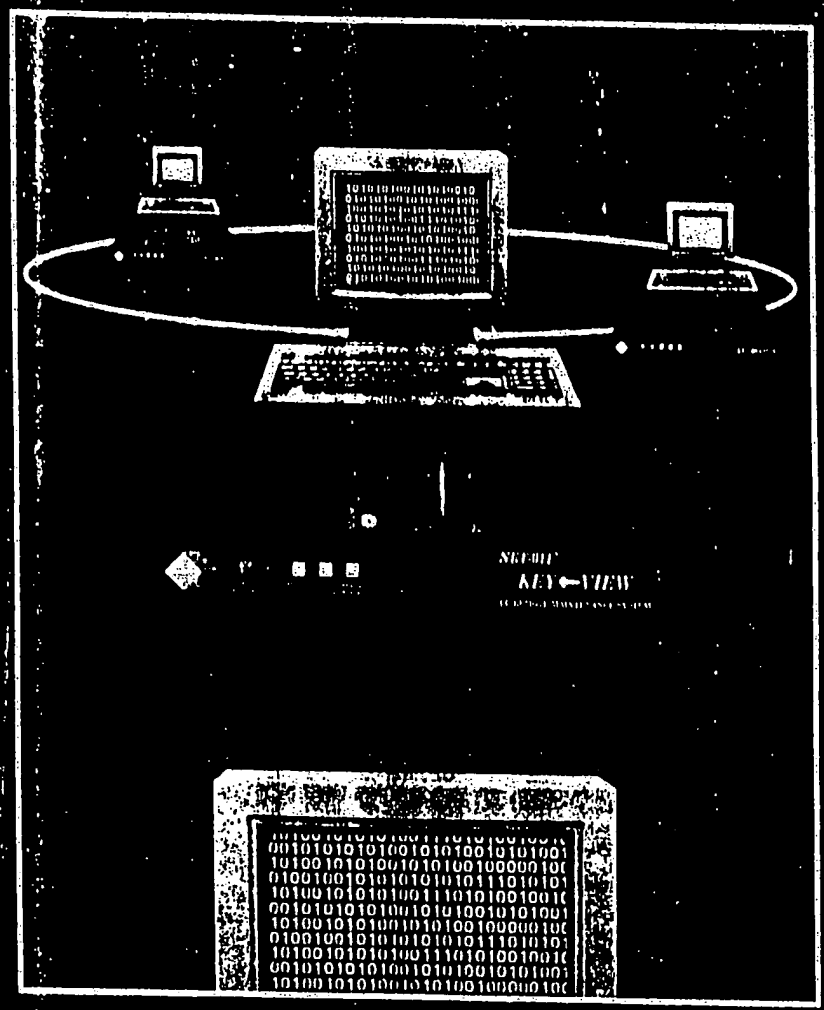

KEY-VIEW™

PC Remote Maintenance System

User's Reference Manual

CY 001021

NET-911 ®

KEY-VIEW SYSTEM

USER'S REFERENCE MANUAL

FOX NETWORK SYSTEMS INCORPORATED
15200 SHADY GROVE ROAD
ROCKVILLE, MARYLAND 20850

REV: 3.3 - July 7, 1994

NOTICES

LICENSE NOTICE

Fox Network Systems Inc. reserves the right to make changes or improvements to the KEY-VIEW System at any time and without notice. The software supplied as part of the KEY-VIEW System is a proprietary product of Fox Network Systems Inc. and is not and has never been free or in the public domain. This is a copyrighted document which may not be reproduced, copied, translated or converted into machine readable media in whole or in part without the prior written consent of Fox Network Systems Inc. There is a patent pending for the KEY-VIEW System. No user may modify KEY-VIEW in any way, including de-compiling or reverse engineering the System. The KVTRAIN.EXE, KVFILE.EXE and other software programs that are intended to operate on the PC attached to a KEY-VIEW unit are licensed for use only on a single Personal Computer (PC) and only in conjunction with the external KEY-VIEW hardware purchased with the System. All other KEY-VIEW software programs may be freely copied to PC's that may remotely access a KEY-VIEW hardware unit, but said software programs may only be used for the purpose of accessing a KEY-VIEW hardware unit. Any modifications to the KEY-VIEW System, its software, hardware or components, not expressly approved in writing by Fox Network Systems Inc. are not permitted, void any and all warranties, and could void the user's authority to operate the equipment.

The KEY-VIEW System consists of both computer hardware and software. You may not copy, create derivative products, modify, reverse engineer or transfer any portion of this system without the express written approval of Fox Network Systems Inc. If you transfer possession of this system to a third party, your license to use this KEY-VIEW System is terminated concurrent with said transfer.

NET-911 is a registered trademark and KEY-VIEW is a trademark of Fox Network Systems Inc. pcAYWHERE is a registered trademark of Symantec Inc. Carbon Copy is a registered trademark of Microcom Inc. Novell and Netware are registered trademarks of Novell Inc. Hayes is a registered trademark of Hayes Microcomputer Products Inc. Windows is a registered trademark of Microsoft Corporation. Other trademarks are the property of their respective owners.

WARRANTIES

Before you use the KEY-VIEW System, please read the following terms and conditions stated in this section as well as the features and limitations of this product contained in this manual. If you do not agree to these terms or this product, as described in this manual, does not meet your needs; do not attempt to use the KEY-VIEW unit or open the enclosed envelope containing the KEY-VIEW software diskettes. Instead, return the complete KEY-VIEW System in it's original packaging to the place of purchase for a refund. Once the enclosed envelope is opened, refunds will not be honored and the product warranty is subject to the specific terms stated herein.

KEY-VIEW is sold on an "AS IS" basis, without any warranty, expressed or implied. The entire risk as to quality and performance of the product is with you, the licensee. Some states do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

Fox Network Systems Inc. (FOX) warrants the KEY-VIEW System to be free of defects in workmanship for a period of one year from the date of purchase. If the KEY-VIEW System has been licensed directly from FOX on a rental basis, FOX warrants the KEY-VIEW System to be free of defects in workmanship for the duration of the rental period. In the event of a defect in a KEY-VIEW System purchased by a customer, Fox Network Systems Inc. will repair or replace the defective part upon receipt of the defective part by Fox Network Systems Inc. along with a corresponding proof of purchase receipt and a return authorization number issued by us. Warranty repairs will not be made in any cases where (1) the tamper seal on the bottom of the KEY-VIEW unit is missing or is damaged or there is other evidence that maintenance was performed on the KEY-VIEW unit by other than Fox Network Systems Inc.; (2) the unit was not installed or used in accordance with the procedures set forth in this manual; or (3) the unit shows signs of physical abuse. Please contact our technical support group for a return authorization number related to any repairs required. Our current technical support phone number is contained in the README.TXT file located on the installation diskette supplied with the KEY-VIEW System.

Fox Network Systems Inc. will not honor any claims resulting from the failure of the user to follow the procedures specified in this manual or any updates thereto contained on the README.TXT file contained on the KEY-VIEW installation diskette. In any event, the remedy for any breach of warranty shall be limited to replacement or repair of the defective part and shall not include any consequential damages, lost profits, lost savings or other incidental damages or claims arising out of any purchaser's or user's use or inability to use the KEY-VIEW System.

Fox Network Systems Inc. does not warrant the product's fitness for a particular purpose nor do we warrant that the product or software supplied with the product contains no defects, or is error free. The KEY-VIEW software programs included on the enclosed diskettes are provided without any warranty either expressed or implied. Damaged diskettes should be returned for replacement. This agreement shall be governed by the Laws of the State of Maryland.

FCC REQUIRED NOTICES

WARNING: This equipment generates, uses and can radiate frequency energy and, if not installed and used in accordance with the instructions manuals, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

TABLE OF CONTENTS

Ref. Description	Page
1.0.0 INTRODUCTION	1
2.0.0 INSTALLATION	9
2.1.0 Installing KEY-VIEW Unit	12
2.2.0 Training KEY-VIEW Unit	19
2.3.0 Installing KEY-VIEW Modem	24
2.4.0 Installing HOST PC Utility Software	25
2.5.0 KEY-VIEW Configuration Changes	31
3.0.0 KEY-VIEW LOCAL PC PROCEDURES	33
3.1.0 KEY-VIEW Overview	34
3.2.0 Setup KEY-VIEW Processing Options	35
3.2.1 Call List Processing	35
3.2.2 Modem Setup	40
3.2.3 Printer Setup	43
3.2.4 Return to Main Menu	45
3.3.0 Calling A KEY-VIEW HOST Unit	45
3.4.0 KEY-VIEW Connection Options	52
3.4.1 Set Display Mode	52
3.4.2 Switch HOST/LOCAL Mode	55
3.4.3 Cold Boot Host	57
3.4.4 Switch Units	59
3.4.5 Unit Maintenance	60
3.4.6 Print Host Screen	65
3.4.7 File Transfer	66
3.4.8 Terminate Call	71
3.4.9 Return to Main Menu	73
3.5.0 Exiting KEY-VIEW	73
4.0.0 VGA GRAPHIC DISPLAYS	75

4.1.0 Microsoft Windows Graphics Interface 77

5.0.0 UNIT STATUS INDICATORS 79

6.0.0 OTHER OPERATING PROCEDURES 81
6.1.0 Coordinating Simultaneous HOST PC Access 81
6.2.0 Hot Keys When Connected to a KEY-VIEW Unit 82
6.3.0 LOCAL PC Keyboard Considerations 83
6.4.0 LOCAL PC Loss of HOST PC Video Screen 84
6.5.0 Access to HOST PC's Hardware Configuration 85
6.6.0 Considerations When Daisy-Chaining Units 86
6.7.0 Other Considerations 86

7.0.0 FREQUENTLY ASKED QUESTIONS 89

8.0.0 ERROR MESSAGES & SUGGESTED ACTIONS 93

9.0.0 APPENDIX 95

10.0.0 INDEX TO KEY-VIEW MANUAL 99

APPENDIX & EXHIBIT INDEX

PAGE

Appendices

A - KEY-VIEW DIP Switch Unit ID Settings 97

Figures

1 - Diagram of KEY-VIEW Unit Rear Panel 12
2 - Training Introduction Screen 21
3 - Training Status Screen 22
4 - KVMODEM.EXE Parameters 27
5 - KEY-VIEW Main Menu 35
6 - Setup Menu Options Screen 36
7 - Call List Entry Screen 37
8 - Call List Help Screen 39
9 - LOCAL PC Modem Setup Screen 40
10 - Printer Setup Screen 43
11 - Call HOST System Menu 46
12 - HOST Connect Options 51
13 - Main Menu Screen When HOST Connection Active 52
14 - Connection Options Menu Screen 53
15 - Display Mode Options Screen 56
16 - HOST/LOCAL Mode Options Screen 57
17 - Cold Boot Confirmation Screen 58
18 - Call List Screen to Switch HOST PCs 60
19 - Password/Access Security Screen 61
20 - HOST PC File Transfer Screen 68
21 - File Transfer Options Screen 69
22 - File Transfer Specifications Screen 70
23 - File Transfer Progress Screen 71
24 - Terminate Call Confirmation Screen 72
25 - Diagram of KEY-VIEW Unit Front Panel 79

1.0.0 INTRODUCTION

The KEY-VIEW System permits a Personal Computer (PC) at a local site ("LOCAL PC") to access and control another PC, regardless of the application being run, at a remote site ("HOST PC"), without Central Processing Unit (CPU) support from the HOST PC. The HOST PC is directly connected to the KEY-VIEW unit which is linked to a LOCAL PC via standard modems and phone lines. The KEY-VIEW unit can be connected to any HOST PC having a standard AT style keyboard and a 9 pin monochrome or 15 pin VGA video interface. The KEY-VIEW System supports remote access in both text and VGA graphics video modes.

The KEY-VIEW System is part of a family of NET-911 products. Each product in the family is designed to perform specific functions that further enhance the usefulness of the entire family, particularly for PC network administration purposes. For example, the NET-911 NETWORK TROUBLE ALERT SYSTEM is a fail safe System that issues custom user recorded voice alerts over the telephone should a network file server fail, power fail, or other designated process fail to operate. Once such an alert call is received, the network administrator could access the failed file server using the KEY-VIEW System, even if the file server is locked up or otherwise inoperable, and then begin to initiate required corrective actions remotely to restore normal processing.

A third member of the NET-911 family, NET-911 SWITCHER, allows switching an AC power source from one power source (e.g. a possibly defective UPS battery backup) to another power source (e.g. another new UPS) without causing a power break. This device could be used to avoid shutting down a network file server when replacing a defective UPS system or adding/removing a new power control device such as KEY-VIEW.

1.0.0 INTRODUCTION

TELEBOOT is the final product in the NET-911 family. TELEBOOT permits remote rebooting of a PC (temporarily cutting AC power to the PC) based on a specific number of phone rings. TELEBOOT is typically used to restore normal PC processing in cases where a HOST PC is running a communications software program, such as pcANYWHERE or Carbon Copy, and has locked up during a remote communications session. TELEBOOT could also be used to remotely access network print servers, communication servers, and other units that may require restarting after a network has failed and then been remotely re-activated using the KEY-VIEW System.

Unlike other remote access systems, the KEY-VIEW System does not need any operating system software to be resident on the HOST PC in order to achieve full remote control over a HOST PC. On this basis the KEY-VIEW System now permits access to a HOST PC in cases where processing has "locked-up" or the HOST PC is running applications that control all memory in a PC or are incompatible with available software based remote access systems (e.g. pcANYWHERE, Carbon Copy, etc.), such as many network operating systems, communications servers, print servers, etc. Moreover, the KEY-VIEW System has the necessary tools for a LOCAL PC to restore normal HOST PC processing in most cases. For example, the KEY-VIEW System could be used to remotely view or change the CMOS setting on a HOST PC! In cases where remote repair may not be possible (e.g. a hard drive is defective), the KEY-VIEW System provides the necessary unrestricted access required to remotely determine what repairs (e.g. replace hard drive) will be necessary to restore normal HOST PC operations.

Most network operating systems do not permit remote access software applications to co-exist with the network file server's operating system. If the file server's operating system fails, the file server's processor locks up for any reason, or the network cabling systems fail, the network administrator will not be able to determine the reason for the failure and effect repairs without having direct, on-site access to the file server. However, if a KEY-VIEW System had been installed on that file server,

the network administrator would have been able to use any LOCAL PC to remotely access the KEY-VIEW unit, view what appears on the file server's screen, physically take over the file server's keyboard, control operations and/or cold boot the file server, as required. The KEY-VIEW System thus provides network administrators with unconditional access to any network PC (HOST PC) without requiring either CPU or Local Area Network (LAN) communications support from the HOST PC or the network.

As an example of other uses for the KEY-VIEW System, consider the case of a law firm where each lawyer in the firm depends on a multi-port network communications server for remote access to their client and legal reference files. If one or more ports on the communications server should fail, remote access to the firm's files and network would not be possible or haphazard. In such cases, simply re-booting the communications server remotely is not desirable because there may be other remote users on ports that are still operating properly, so "blindly" rebooting the communications server would immediately cut off their connection(s). Obviously, a network administrator must be in a position to take immediate corrective action, but need not be on-site. KEY-VIEW now permits administrators to remotely access and control the communications server immediately, as if they are physically sitting in front of the server.

KEY-VIEW may also be used for more efficient remote maintenance of PCs. When a failure occurs, personnel on-site could simply connect a spare KEY-VIEW unit to the failed PC, thereby permitting a remote maintenance center to take over the PC for purposes of running diagnostic procedures. In many cases the problem may be correctable remotely by the maintenance center, thus avoiding wasted technician travel time. At a minimum KEY-VIEW provides management personnel with the information necessary to know what parts and technician skill levels are required to make the on-site repairs before anyone is dispatched to the site.

As a final example, KEY-VIEW may be used to remotely monitor user activities to significantly enhance network security. For example, a bank

could connect a KEY-VIEW unit to each PC in a remote branch and daisy-chain the units together so that one modem and phone line could be used to remotely monitor the activities of each PC in the branch from a separate site, such as a central maintenance center. Units acquired for this purpose would not have status indicators. As a result, branch staff would have no way of knowing whether or not their PC was being monitored remotely. More importantly, the monitoring process would have no effect on normal PC operations. In cases where monitoring was intended primarily as a deterrent to possible abuse, some of the KEY-VIEW units installed could be low-cost, phantom units.

The typical KEY-VIEW System configuration consists of four major components:

(1) The KEY-VIEW unit - a hardware unit that is directly connected to the HOST PC;

(2) HOST PC software - used initially to train the KEY-VIEW unit to properly decode the video output signal of the HOST PC;

(3) LOCAL PC software - permits the LOCAL PC via modem to remotely access a KEY-VIEW unit and control the HOST PC connected to the unit; and

(4) HOST site modem - permits access to each HOST PC at that site (up to a total of 60 PCs per modem).

A KEY-VIEW unit is directly connected to a HOST PC. Since the unit is an external, stand-alone hardware device; it takes only minutes to install. The PC video, keyboard and AC power cables simply connect to and past through the KEY-VIEW unit, thereby permitting the unit to:

(1) Re-direct keyboard input to a LOCAL PC, when required;

(2) Receive and decode the HOST PC's video output signal so that the video screen can be viewed remotely without processor support from the HOST PC; and

(3) Control AC power to the HOST PC so that a remote user can request that AC power to the HOST PC be interrupted, forcing the HOST PC to "cold-boot".

A KEY-VIEW unit may be directly connected to a modem or daisy-chained through another KEY-VIEW unit to the modem. In this latter case, linking multiple units together permits a remote user to access and control multiple HOST PCs using a single phone line during a single access session. In other words, a remote user may freely switch between HOST PC's from a single LOCAL PC simply by issuing commands on the LOCAL PC. Currently, up to 60 units may be daisy-chained together. The KEY-VIEW System eliminates the need to purchase costly "hard-wired" switching devices with complex and costly direct cabling requirements to control multiple PCs from a single PC. The KEY-VIEW System also eliminates the need to purchase monitors and keyboards for HOST PCs, if they are not otherwise required.

KEY-VIEW communication interfaces use moderate cost, easy to install RJ-45 (8 wire), flat, "straight-through" cable. Special adapters are provided with KEY-VIEW to interface the RJ-45 cabling to modems or standard HOST PC serial ports. The maximum distances that RJ-45 cable may be run between KEY-VIEW units, between a KEY-VIEW unit and a modem, or a between KEY-VIEW unit and an associated HOST PC is 250 feet. There is no restriction as to the total length of all RJ-45 cable in a daisy-chain, as long as the cable has "straight-through" wiring. Optional inexpensive adapter cables are available to convert from RJ-45 cable to RJ-11 cable, so that existing telephone wire can be used to daisy-chain one KEY-VIEW unit to another KEY-VIEW unit.

The KEY-VIEW System must be adapted to the HOST PC and the video card which is installed therein. To accommodate this process, the KEY-

VIEW software must be installed and run on the HOST PC to train the KEY-VIEW unit to recognize the video output of the HOST PC's video card. Such software should be run before attempting to remotely access the HOST PC. This software causes various screens to be displayed on the HOST PC that permit the KEY-VIEW unit to adapt itself automatically to the specific video output of the HOST PC. This process is used only to initialize the system. It should be run after the unit is initially installed and whenever the HOST PC video card or cable between the video card and KEY-VIEW unit is changed. Accordingly, this training software need not be installed or remain on the HOST PC's hard disk.

KEY-VIEW units operate best using a Fox Network Systems recommended video card that is available as an option at the time of purchase. These video cards are available to support either 9 pin monochrome monitors or 15 pin VGA monitors at a nominal price (i.e. less than $50). Acquiring and installing these video cards with the KEY-VIEW System is strongly recommended. This simplifies the installation procedure, and ensures the greatest degree of reliability when remotely accessing a HOST PC.

If the optional video card is not used, the KEY-VIEW System will still adapt itself to most existing HOST PC video cards, since video output signals follow a fairly rigid standard to interface with a large variety of commercially available video monitors. However, many of the older model video cards have erratic, noisy or weak output signals that may impair the ability of the KEY-VIEW System to reliably decode the signal. In rare cases, it may not be possible to train the KEY-VIEW unit to recognize the output signals of a video card. In such cases, the KEY-VIEW training process will halt indicating the video card is not compatible. If this should occur, Fox Network Systems will swap the non-compatible video card for a compatible video card free of charge. Fox Network Systems evaluates all such incompatible cards to identify enhancements that could resolve such compatibility problems in the future.

LOCAL PC software is provided with the KEY-VIEW System permitting a LOCAL PC to access the KEY-VIEW unit and HOST PC. This software may be freely installed on as many LOCAL PC's as may be needed to access KEY-VIEW units. No additional license fees apply to each copy of such software installed on a LOCAL PC.

Software is provided to permit a HOST PC to modify the modem setup string used by a KEY-VIEW unit to initialize a modem connected to the unit and to permit file transfers to occur between a LOCAL PC and a HOST PC via one of the HOST PC's serial ports. This software is only invoked when necessary and is not needed in memory for the KEY-VIEW System to operate and enable a LOCAL PC to access and control a HOST PC.

To prevent unauthorized access by LOCAL PC's to KEY-VIEW units, all KEY-VIEW unit access is controlled by passwords. Initially, KEY-VIEW units are shipped with the default password set to "KEYVIEW", which must be specified using only capital letters, and no hyphen. After the installation process is complete, the password may be changed by any remote user after they have successfully accessed the unit using "KEYVIEW" as the password. Once a password has been changed, the unit cannot be accessed until the correct password is entered by a remote user. Passwords used may contain either alphabetic and/or numeric characters and are case sensitive. If the password is forgotten or lost, the unit must be returned to Fox Network Systems to reset the password (in which case a handling fee will be incurred). This approach precludes users gaining unauthorized access to a HOST PC by tampering with the KEY-VIEW unit to restore it's default password.

Passwords are encrypted when transmitted from a LOCAL PC to a KEY-VIEW unit in such a manner as to prevent someone tapping into the phone line to view or decipher the password. In addition, as part of the configuration process for a KEY-VIEW unit, remote users may be limited as to the number of password guesses that may be made before they are locked out of a KEY-VIEW unit. Such lock-outs may be set only for the

current access session and/or may be set to remain in effect until someone depresses the "ACTION" button located on the front of the KEY-VIEW unit. Depressing the "ACTION" button will reset the lock-out feature but will not allow remote access without the correct password.

Once the KEY-VIEW System has been connected to a HOST PC, the HOST PC need not have either a monitor or keyboard unless there is still a need to access the HOST PC on site. Many customers like this feature of the KEY-VIEW System because it improves network security by precluding employees tampering with critical network operating systems, saves the cost of keyboards and monitors, saves space and power needs in cramped computer rooms, and eliminates the need for costly keyboard and monitor switch boxes. In cases where VGA monochrome monitors remain connected to a HOST PC, LOCAL PC's with color monitors may access the HOST PC in a color mode even though only a VGA monochrome monitor is connected to the HOST PC!

2.0.0 INSTALLATION

Before proceeding with any of the installation steps for the KEY-VIEW System please print out and carefully review the contents of the README.TXT text file included on the KEY-VIEW Installation diskette. To print the contents of this file insert the installation disk into drive A:, make sure the work station used has access to a printer and the printer is ready, and then at a DOS prompt enter:

TYPE A:\README.TXT > PRN

The README.TXT file contains information on late breaking news, product updates and enhancements.

Each basic KEY-VIEW System is shipped with the following items:

1 - KEY-VIEW unit
1 - 3.5" KEY-VIEW Installation Diskette
1 - AC power adapter cord
1 - RJ-45 to 25 pin male adapter plug (for modem)
1 - RJ-45 to 9 pin female adapter plug (for HOST PC serial port)
2 - 7 ft RJ-45 interface cables (for modem/serial port)
1 - 9 pin male to 25 pin female converter plug (for modem/serial)
1 - Unit to PC male to male keyboard interface cable
1 - Unit to PC 9 pin male to female non-VGA video interface cable

NOTE: *Sites using the 6 pin mini-keyboard (i.e PS-2, Compaq style keyboard) connectors will need the optional keyboard interface adapter plug set to connect the keyboard to the KEY-VIEW unit and connect the KEY-VIEW unit to the HOST PC. Other optional connectors are also available from Fox Network Systems, as follows:*

- 9 pin male to female gender changer
- 25 pin male to female gender changer
- RJ-45 to 9 pin female adapter plug (for direct connect)
- RJ-45 to RJ-11 adapter

In cases where the optional VGA interface is installed in the KEY-VIEW unit, the KEY-VIEW System will also include a KEY-VIEW unit to PC 15 pin male to male VGA video interface cable.

Please verify that the above items are included with your KEY-VIEW System before proceeding with the installation process. The converter plug supplied with the KEY-VIEW System may not be necessary for most installations, but is provided to handle situations where it may be necessary to interface the KEY-VIEW unit with a 25 pin serial port on a HOST PC or 9 pin serial interface receptacle on a modem.

The Installation diskette provided with the KEY-VIEW system is only available in a 3.5" media. If a 5.25" diskette is needed, simply copy the entire contents of the Installation diskette from the 3.5" disk to a 5.25" diskette using the DOS XCOPY command.

After unpacking the KEY-VIEW unit make sure the KEY-VIEW ON/OFF switch located on the right rear side of the KEY-VIEW unit is in the OFF position (by pressing the lower half of the ON/OFF switch before proceeding with the installation process.)

Important: ***Do NOT connect a telephone line to any of the jacks on the back of the KEY-VIEW unit. These jacks are used only to connect the KEY-VIEW unit to a modem, the HOST PC, or to another KEY-VIEW unit. Telephone lines carry voltage that may damage the KEY-VIEW unit and void your warranty. The telephone line used by the KEY-VIEW System should be connected only to the modem as described in this section.***

The HOST PC's keyboard and monitor need not be re-connected to a KEY-VIEW unit after installation of the KEY-VIEW unit. Many users prefer to improve computer room security by permitting access to HOST PC(s) using only the password protected KEY-VIEW System. Other users like the idea of saving the cost of keyboards and monitors, and the power and space required for keyboards and monitors in cramped computer rooms.

A KEY-VIEW unit cannot be connected to the output ports of a central keyboard/monitor switch box. The unit must be connected directly to the video and keyboard output ports of the HOST PC, as described below. The KEY-VIEW unit is sensitive to any changes in the (1) the video cable between the HOST PC and KEY-VIEW unit or (2) video card used in the HOST PC. Accordingly, the unit will not function properly if a switch box is used to switch between HOST PCs. However, the video and keyboard output of a KEY-VIEW unit may be connected to an input port of a switch box instead of directly to a keyboard and monitor.

The KEY-VIEW System permits daisy-chaining multiple KEY-VIEW units together for central access to several HOST PCs as well as the capability to switch between them. Accordingly, many users conclude that PC switch boxes are no longer necessary and simply eliminate them from their system, after the KEY-VIEW units have been installed.

As part of the installation process, the AC power cord used to provide power to the HOST PC is removed from the HOST PC and used as the AC input power cord for the KEY-VIEW unit. In order to comply with part 15 of FCC regulations this power cord must be shielded to prevent emissions. If the cord is not shielded, make sure to replace this cord with a shielded power cable, immediately.

After the installation process is complete, whenever the video card in the HOST PC is changed, the cable between the video card and KEY-VIEW unit is changed or a new HOST PC is connected to a KEY-VIEW unit; the KEY-VIEW unit may need to be re-trained as more fully described in sections 2.2.0 and 2.4.0.

2.1.0 Installing KEY-VIEW Unit

As the first step in the KEY-VIEW installation process, the HOST PC to which the KEY-VIEW unit will be attached should be selected. This HOST PC should be an IBM compatible PC having either a 9 pin monochrome or 15 pin VGA video interface card and a standard AT compatible keyboard. During the installation process, the HOST PC selected will need to be turned OFF to connect the KEY-VIEW AC power cable to the HOST PC. Also, the HOST PC will need to invoke the DOS operating system in order to run the KVTRAIN.EXE program to train the KEY-VIEW unit to recognize the HOST PC's video card output signals. In cases where the hard drive used to boot the HOST PC does not have a DOS partition, the HOST PC will need to be booted from a floppy disk containing DOS in order to invoke the KVTRAIN.EXE program.

After a HOST PC has been selected, connect the various cables provided with the KEY-VIEW System to the rear panel of the unit. The layout of the KEY-VIEW unit's rear panel is illustrated in Figure 1.

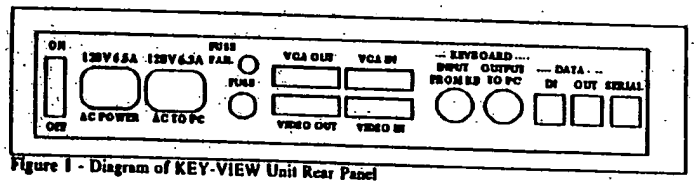

Figure 1 - Diagram of KEY-VIEW Unit Rear Panel

One end of the male to male keyboard interface cable should be plugged into the female "KEYBOARD OUTPUT TO PC" connector located on the back of the KEY-VIEW unit.

If the KEY-VIEW unit is to be connected to a HOST PC with a 15 pin VGA video interface cable, then plug one end of the 15 pin male to male interface cable into the optional 15 pin female "VGA IN" connector located on the back of the KEY-VIEW unit. Otherwise, plug the female end of the 9 pin male to female video interface cable into the 9 pin male "VIDEO IN" connector located on the back of the KEY-VIEW unit.

Connect the end of one of the RJ-45 cables provided into the RJ-45 jack on the back of the KEY-VIEW unit labeled "DATA IN". Connect the end of the other RJ-45 cable provided into the RJ-45 jack labeled "SERIAL" on the back of the KEY-VIEW unit.

Next, the KEY-VIEW unit cables must be connected to the HOST PC. Before connecting these cables, the HOST PC's ON/OFF power switch must be turned OFF. In cases where a KEY-VIEW unit is connected to a network file server or other PC that may be impractical to turn OFF, it is suggested that a NET-911 SWITCHER unit be purchased and placed between the HOST PC and the KEY-VIEW unit. This approach permits removing the KEY-VIEW unit for repair or replacement without the need to interrupt HOST PC processing. The NET-911 SWITCHER unit permits changing from one AC power source to another AC power source without interrupting HOST PC processing.

Several steps are required to connect the KEY-VIEW cables to the HOST PC as follows:

(1) Unplug the HOST PC's keyboard from the HOST PC. Then, plug the keyboard's plug into the "KEYBOARD INPUT FROM KB" receptacle on the back of the KEY-VIEW unit. Next, plug the male end of the "KEYBOARD OUTPUT TO PC" cable into the keyboard input receptacle located on either

the back or front of the HOST PC.

NOTE: *Users with "mini" keyboard connectors, such as those used on IBM PS 2 and Compaq PCs, will need two optional connector adapters to plug the keyboard into the KEY-VIEW unit and to connect the KEY-VIEW unit to the HOST PC's keyboard input receptacle. These optional adapters are available from Fox Network Systems.*

(2) Unplug the HOST PC's video cable (connected to the PC's video display monitor) from the HOST PC's video output card and plug the cable into either the 9 pin "VIDEO OUT" or 15 pin "VGA OUT" receptacle on the back of the KEY-VIEW unit depending on the number of pins on the video cable connector.

NOTE: *In cases where the optional VGA card is installed in KEY-VIEW unit, do not attempt to connect both a 15 pin and 9 pin video display monitor into the KEY-VIEW unit at the same time. Also, any video display monitor connected to the unit must match the HOST PC's video display adapter card. In other words, if the unit's "VIDEO IN" port is used, only a monochrome monitor with a 9 pin connector at the end of the video cable should be connected into the unit's "VIDEO OUT" port. Similarly, if the unit's "VGA IN" port is used, a VGA video monitor must be connected to the unit's "VGA OUT" port.*

(3) Plug the open end of the cable previously connected to either the "VIDEO IN" or "VGA IN" receptacles on the back of the KEY-VIEW unit into the HOST PC's video output receptacle located on the back of the HOST PC.

(4) Plug the open end of the RJ-45 cable previously connected to

the "SERIAL" receptacle on the back of the KEY-VIEW unit into the RJ-45 jack on the 9 pin female serial interface adapter. Then, plug the female (9 pin) side of the connector into an available serial port on the HOST PC. If the only serial port available on the HOST PC is 25 pin, then use the 9 pin male to 25 pin female converter plug supplied to connect the cable to the HOST PC's serial port.

NOTE: *A serial connection from the KEY-VIEW unit to the HOST PC is optional and is only used to change the KEY-VIEW unit's default modem setup commands or to use the file transfer feature of the KEY-VIEW System, which permits files to be transferred from a LOCAL PC to the HOST PC. To insure file transfers will be possible in emergency situations where critical HOST PC files may have been corrupted or lost, it is strongly recommended that this serial connection always be installed and tested.*

(5) Unplug the HOST PC's AC power cord from the HOST PC. Then, plug this cord into the "AC POWER" receptacle on the back of the KEY-VIEW unit. In order to comply with part 15 of FCC regulations this AC power cord must be shielded to prevent emissions. If the cord is not shielded, replace this cord with a shielded power cable.

(6) Plug the special AC power cord supplied with the KEY-VIEW unit into the "AC TO PC" receptacle on the back of the KEY-VIEW unit. Then, connect the other end of the AC power cord to the HOST PC's AC power input receptacle. If a NET-911 SWITCHER unit is to be installed, then plug the other end of the AC cord supplied with the unit into the "AC MAIN INPUT" receptacle on the SWITCHER unit, plug the SWITCHER unit's AC power cord into the AC OUT receptacle on the SWITCHER unit, and plug the other end of

the SWITCHER unit's AC power cord into the AC input receptacle on the back of the HOST PC.

(7) Connect the remaining open end of RJ-45 cable attached to the "DATA IN" jack on the back of the KEY-VIEW unit into either the "DATA OUT" jack of another KEY-VIEW unit or to an external, stand alone, Hayes compatible modem, using the RJ-45 to 25 pin male adapter provided. When a KEY-VIEW unit is connected to another unit, at least one of the KEY-VIEW units on the daisy-chain must be connected to a modem, if remote access is desired. The modem connection can be accomplished by connecting the open end of the RJ-45 cable into the RJ-45 to male 25 pin adapter. Then, plug this adapter into the serial data output interface receptacle on the modem. If the modem has a female 9 pin receptacle, then use the 25 pin female to 9 pin male converter plug supplied with the KEY-VIEW System to complete the unit-to-modem connection. After the connection to the modem is completed, connect the modem to an AC power source, then turn the modem ON.

NOTE: *A daisy-chain of KEY-VIEW units may be connected directly to a LOCAL PC instead of through a modem. This approach should only be used in cases where remote access over phone lines is not desired and the optional "direct connect" adapter has been purchased. Direct connection permits a single LOCAL PC at a site to control multiple HOST PC's on site using a dedicated RJ-45 line. To accomplish direct connection (1) no KEY-VIEW unit on the daisy-chain should be assigned as unit 00 and (2) the first unit on the daisy-chain should be connected directly to the LOCAL PC's serial port by connecting the RJ-45 cable from the unit's DATA IN receptacle to the RJ-45 jack on the optional 9 pin female direct connect adapter, then plug this adapter into the LOCAL PC's serial port, which may also require the use of a*

9 pin male to 25 pin female converter plug. When direct connection is used, the modem type option in the KEY-VIEW modem setup process must be set to "Direct Connect" as discussed in section 3.2.2.

(8) Look at the 8 DIP switches located on the left rear side of the KEY-VIEW unit. The left 6 switches indicate the unit's ID. These 6 switches should all be in the down position (unit ID 00 - factory default), if the KEY-VIEW unit is connected directly to a modem. Otherwise, when the unit is daisy-chained through other units, each KEY-VIEW unit on the daisy-chain must be assigned a unique address from 1 to 59. On this basis, a maximum of 60 units can be daisy-chained to a single modem. These 6 switch settings represent binary values reading from left to right. Accordingly, if only the left most DIP switch is set to the UP position, the unit ID would be 1. If the left most two switches were set to the UP position, the unit ID would be 3, (i.e. 1+2) and so forth. Appendix A contains a complete list of the decimal value (i.e unit ID) for all possible combinations of DIP switch settings. In order to remotely access a KEY-VIEW unit, the unit ID must be correctly defined on the remote PC's call table, as discussed later in this manual. KEY-VIEW units may not be accessible remotely if any unit IDs (i.e. switch settings) on a daisy-chain are not unique, the unit connected to the modem is not set to unit ID 00, or an incorrect unit ID is specified when attempting to access a particular KEY-VIEW unit remotely!

DIP switch 7 is used to set the type of VGA monitor that is connected to the KEY-VIEW unit. If a monochrome VGA monitor or a non-VGA monitor is connected to the unit, this DIP switch should be in the DOWN (default) position. If a color VGA monitor is connected to the unit, this DIP switch should be in the UP position.

DIP switch 8 permits KEY-VIEW to handle non-standard keyboards. *Some PC Manufacturers have recently adopted keyboards with new Scan Codes that are not downward compatible with typical PC keyboards in use.* One such example is the IBM MODEL 95. As explained in section 2.2.0, if KEY-VIEW unit training should fail immediately or lock up, it is possible that one of these new keyboards is in use. To resolve this problem, turn the KEY-VIEW unit OFF, place DIP switch 8 on the side of the KEY-VIEW unit to the UP position, turn the KEY-VIEW unit ON, reboot the HOST PC, then attempt to re-start the training process on the HOST PC. Otherwise, leave DIP switch 8 in the DOWN position.

(9) Turn the ON/OFF switch located on the right, rear side of the KEY-VIEW unit to the ON position by pressing the upper half of the switch. At this point the POWER indicator light on the front of the KEY-VIEW should be ON.

NOTE: *When a KEY-VIEW unit is turned OFF, the video display monitor connected to the KEY-VIEW unit will go blank. This occurs because each KEY-VIEW unit intercepts and processes the HOST PC's video signal then passes it through to the HOST PC video monitor. Also, when the unit is turned OFF, any unit daisy-chained to the unit's DATA OUT port will no longer be accessible remotely as discussed in more detail in section 6.6.0.*

Important: *It is strongly recommended that the modem used by the KEY-VIEW System be connected directly to a telephone company service (i.e. a TELCO jack) instead of a PBX or other type of private phone switching system. Such switching systems could fail if power fails, which would prevent any phone access to the KEY-VIEW System!*

An optional adapter may be purchased to permit KEY-VIEW

units to be daisy-chained using standard RJ-11 telephone cable. If such adapters are used, the heads must be installed on the ends of the RJ-11 cable so that straight-through wiring is achieved from head to head. Most standard telephone cable heads are installed so as to reverse lines between the connectors. These type of cables will not work unless one of the heads is cut-off and replaced with a head that is rotated 180 degrees, so that straight through wiring is achieved from head to head.

2.2.0 Training KEY-VIEW Unit

In cases where the KEY-VIEW optional video card has been purchased and installed in the HOST PC, it will not be normally necessary to train the KEY-VIEW unit to recognize the video card and this section (2.2.0) may be skipped. However, it is usually a good practice to re-train the KEY-VIEW unit regardless of the video card used. In rare situations it is possible that video distortions may occur that require the KEY-VIEW unit to be re-trained. In such cases, follow the procedures in this section to re-train the KEY-VIEW unit before calling for technical support.

Decoding the video output of a PC is a complex process. Before a KEY-VIEW unit can be accessed remotely, it must be trained to recognize the specific video output signal of the HOST PC to which the unit is connected. Video output signal quality may vary based on the video card installed in the HOST PC. Also, the bits (i.e pixels) used to configure characters on a video display monitor may vary from video card to video card. On this basis, whenever the video card installed on the HOST PC is switched, the KEY-VIEW unit must be re-trained, even if the switch involves using the same brand and model video card and/or monitor! Once a unit has been trained, the specific procedures required to decode the HOST PC's video signal are stored in the unit's non-volatile memory. Information stored in non-volatile memory is saved even if all AC power is removed from the unit, so it is normally not necessary to train a unit more than once.

The KEY-VIEW training process takes about 20 minutes to complete for VGA (15 pin) video display cards and about 25 minutes for monochrome (9 pin) cards. The first step in the training process is to run the KVTRAIN.EXE program from a DOS prompt on the HOST PC. In cases where a HOST PC does not boot to DOS, such as may be the case for a dedicated network server, the HOST PC should be booted from a DOS floppy diskette.

The KVTRAIN.EXE program is included on the KEY-VIEW Installation diskette. This KVTRAIN.EXE program may either be initiated directly from the installation disk or from the HOST PC's hard drive, after copying the KVTRAIN.EXE program to the HOST PC's hard drive. To start the KVTRAIN program, go to the drive and directory where the KVTRAIN.EXE program is located and at a DOS prompt type KVTRAIN, then press the Enter key. A screen similar to that shown in Figure 2 will appear on the HOST PC's monitor.

After the above training screen appears, press and hold the "ACTION" button on the front of the KEY-VIEW unit for about 5 seconds until the KEY-VIEW unit beeps. After a few seconds a new screen should appear on the HOST PC's monitor. If the KEY-VIEW unit is connected to a VGA graphics card, one or more graphical screens will be displayed for approximately one minute per screen. The content of these graphical screens is not important and is only relevant if technical support becomes necessary should the VGA training process fail repeatedly. After these graphical screens are displayed, a screen similar to that shown in Figure 3 appears on the HOST PC. This screen will also be the first screen that appears when the KEY-VIEW unit is connected to a 9 pin, non-VGA card.

When the training process is first initiated, the KEY-VIEW unit identifies the exact character set pixel configuration used by the HOST PC's video card. This process will take several minutes.

After the specific character pixel configuration has been identified, the vertical bar, which is positioned on column 1 of the screen, begins moving across the screen, slowly, one column at a time. During this process, the

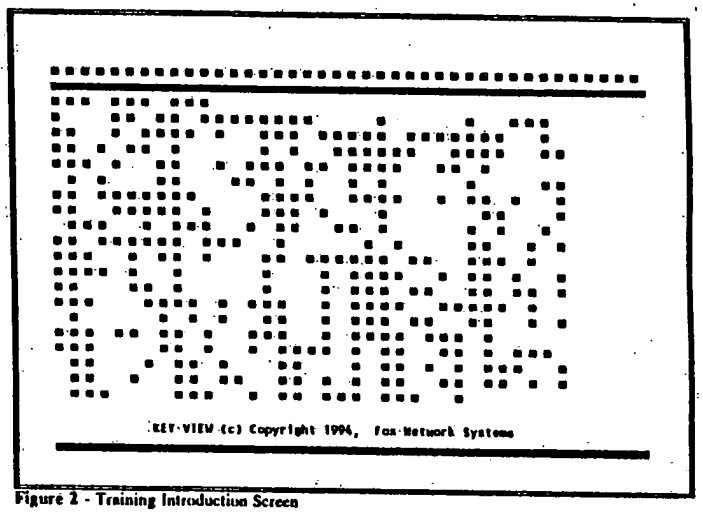

Figure 2 - Training Introduction Screen

KEY-VIEW unit determines the specific vertical video alignment for each column. The Scan Status indicates the column number currently being tested. In cases where signal abnormalities prevent precise determination, the "Current" accumulator (i.e. column error counter) and the "Total" accumulator are incremented by 1, then the KEY-VIEW unit retries the verification process for the column. The "Current" accumulator is cleared each time processing for a new column begins. If after 10 attempts, the alignment for a particular column cannot be determined, the training process is aborted. In this case, the training process can be repeated to see if the problem is correctable. Before repeating the training process, make sure the HOST PC's video card is properly seated in it's bus slot within the HOST PC. If the problem is still not correctable, which is rare, a video card, certified to work with KEY-VIEW, can be obtained from Fox Network Systems either at a nominal charge or the incompatible video card may be swapped for a compatible card free of charge. In the

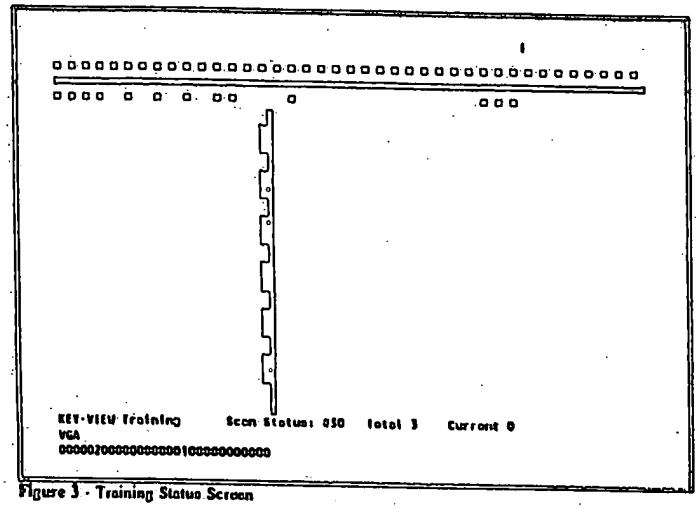

Figure 3 - Training Status Screen

latter case, Fox Network Systems evaluates any incompatible cards received to identify enhancements that may resolve similar compatibility problems in the future.

Once a column has been verified by the KVTRAIN.EXE software, a number from 0 to 9 appears below the column indicating the number of retries that occurred during column verification, then the vertical bar on the screen moves one column to the right. Normally, no more than 2 or 3 total retries (for all columns) should occur during this phase of the training process and typically no retries occur. When the training process is complete, a box appears indicating the total retries that occurred (i.e. "Scan Factor") during the training process. If more than a total of 10 retries occur, consideration should be given to using a certified video card. If a large number of retries occur during training, it is likely that invalid characters (i.e. "garbage") may randomly appear on the LOCAL PC

screen during a remote access session. Normally, this "garbage" consists of solid blocks appearing on the LOCAL PC's screen in place of characters.

After column training is complete, KEY-VIEW checks the video pixel alignment for graphics displays (VGA cards only) and briefly displays and verifies the decoding process for the entire ASCII character set. Both of these processes take less than a minute to complete. Once these tests are complete, the training process is done and KEY-VIEW displays a message on the HOST PC's video display monitor confirming the training process has been successfully completed (including a recap of the number of retries that occurred, as previously discussed). At this point the training process should be ended by pressing the Esc key twice, which causes processing to return to the DOS prompt.

The training process may be aborted by pressing the Action button on the front of the unit and then pressing the Esc key twice on the HOST PC. After this procedure is followed, HOST PC processing will return to DOS.

The training process may be re-run as often as desired by repeating the above procedures. As mentioned, the training process must be re-run whenever the video card used by the HOST PC is changed. The video decoding procedure used by the unit is only updated after the training process has been successfully completed. If the training process has been aborted or failed due to excessive retries, the last successful training results are still retained and used by the unit for video signal decoding.

Important: *Some PC Manufacturers have recently adopted keyboards with new "Scan Codes" that are not downward compatible with typical PC keyboards in use. One such example is the IBM MODEL 95. If training should fail immediately or lock up, it is likely that one of these new keyboards is in use. To help resolve this problem, place DIP switch 8 (i.e. the right most DIP switch) on the side of the KEY-UNIT to the UP position,*

turn the KEY-VIEW OFF then ON, then attempt to re-start the training process on the HOST PC.

In some cases, a HOST PC's video processor may be integrated into the HOST PC's motherboard. If training should fail on such PC's or video decoding mistakes appear frequently when attempting to access the KEY-VIEW unit; procedures normally exist to disable the video processor so that one of the recommended video cards can be installed. However, some manufacturers, such as IBM, may not permit one of these video cards to be inserted into the HOST PC. In such cases, a different PC should be setup, if possible, as the HOST PC.

2.3.0 Installing KEY-VIEW Modem

When a KEY-VIEW unit is connected directly to a modem (as opposed to daisy-chained to another KEY-VIEW unit), the unit ID must be set to 00 (i.e. DIP switches 1 to 6 located on the side of the KEY-VIEW unit are set to the DOWN position).

Important: *It is strongly recommended that the modem used by the KEY-VIEW system be connected directly to a telephone jack (i.e. a dedicated TELCO jack) instead of a PBX or other type of private phone switching system. Such switching systems could fail if power fails, which would prevent any phone access to the KEY-VIEW System!*

All RJ-45 cable used to connect KEY-VIEW units together on a daisy-chain or to connect unit 00 to a modem must be wired on a straight-through basis from connector to connector.

The modem should be plugged into the same AC power source (i.e. wall outlet) used by KEY-VIEW unit 00 to which the modem is to be connected. Using the same AC power source

prevents a situation where AC power is cut to modem but not KEY-VIEW unit 00, which would prevent the modem from being properly re-initialized by the KEY-VIEW unit answering a call.

Presently, the KEY-VIEW unit supports only modems that are totally Hayes compatible. The KEY-VIEW System has been successfully tested on several popular brands of modems as set forth in the README.TXT file located on the KEY-VIEW Installation diskette.

It is strongly suggested that one of the modems listed in the README.TXT file be selected for the KEY-VIEW System at both the HOST and LOCAL sites. As additional modems are successfully tested with the KEY-VIEW System, they will be added to the README.TXT file. Ideally, the same brand/model modem should be connected to KEY-VIEW unit and all LOCAL PC's that may access the unit. Modems with less than a 2400 baud rate are not supported.

When the modem connected to KEY-VIEW unit number 00 is initialized by the unit, the Auto Answer light (i.e the AA indicator) on the front of the modem will be OFF. Unlike most modem applications, the KEY-VIEW unit handles the carrier detect process directly, as opposed to having the modem answer and handle an incoming call. This approach is necessary to help insure that KEY-VIEW units always reset themselves whenever a phone connection is terminated.

2.4.0 Installing HOST PC Utility Software

No software needs to be installed on a HOST PC to permit a LOCAL PC to access and control the HOST PC. However, four utility programs, KVMODEM.EXE, KVFILE.EXE, KVWAIT.EXE, and COM911.EXE should be copied from the KEY-VIEW Installation diskette's directory named "HOST" to a DOS directory (normally named KV or KEYVIEW) on the HOST PC's hard disk drive.

KVMODEM.EXE may be used on a HOST PC attached to a KEY-VIEW unit that is connected to a modem (i.e. a unit with an ID of 00). When KVMODEM.EXE is run on a HOST PC, the program permits the modem setup string to be modified to accommodate different types of modems and to change various modem parameters, such as the number of rings the modem should wait before answering a call. Normally, most modems do not require special setup strings to handle incoming calls from LOCAL PC's. Known modifications required to specific brands of modems are contained in the README.TXT file on the KEY-VIEW Installation diskette.

Some HOST PCs may not have a DOS partition on the PC's hard drive necessary to run the KVMODEM.EXE software. In such cases, a DOS floppy boot diskette should be created, the KEY-VIEW utility programs copied to this boot disk and the disk should be used to re-boot the HOST PC to DOS. Then, run the KVMODEM.EXE program directly from the boot diskette.

Once the KVMODEM.EXE program has been copied, the program and serial linkage between the HOST PC and KEY-VIEW unit can be initiated by invoking the program using the command "KVMODEM COMx". The "x" in the command indicates the HOST PC's serial port number to which the KEY-VIEW unit is connected and the "x" must be replaced with a number from 1 to 4. If the linkage is successful, the screen illustrated on Figure 4 appears. In this case the serial port number to which the KEY-VIEW unit is connected is stored in a file called "KVPORT.DAT, so there is no need to re-specify this port when re-executing the KVMODEM.EXE program.

If the COM port number is not specified or is specified incorrectly, the error message "<< COM PORT HAS NOT BEEN SPECIFIED >>" is displayed on the HOST PC. If the KEY-VIEW unit is not properly connected to the serial port specified, the message "<< KEY-VIEW NOT FOUND >>" is displayed on the HOST PC. Should this error message appear, it is likely (1) there is a serial port interrupt conflict, (2) the serial cable is not properly connected between the KEY-VIEW unit and

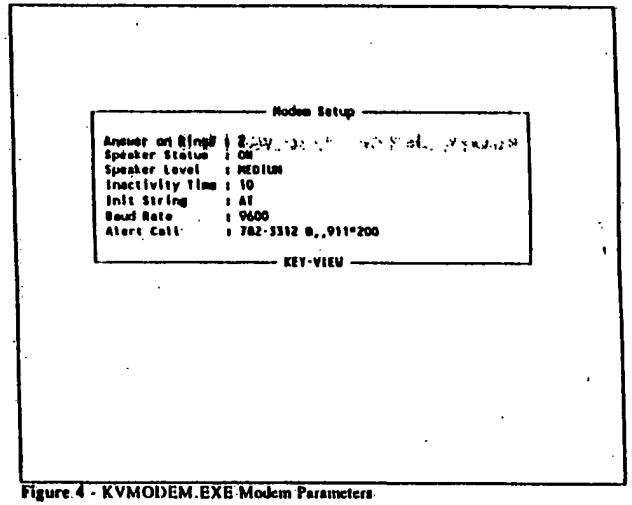

Figure 4 - KVMODEM.EXE Modem Parameters

HOST PC or is defective, (3) the serial port on the HOST PC has been disabled, or (4) the serial port on the unit and/or HOST PC is defective. Completing a proper serial connection between the HOST PC and KEY-VIEW unit is discussed in section 2.1.0. As a possible first step in attempting to resolve the error, try using a different serial port on the HOST PC and/or disable any serial devices on the HOST PC. Then, repeat the test until the linkage can be successfully completed. In some cases a serial port conflict with other devices such as a network card, may exist which causes the HOST PC to lock up after the KVMODEM.EXE program is run. If this should occur, run the COM911.EXE program from a DOS prompt to determine what serial ports exist and if any conflicts were detected.

Advanced users may specify alternative serial port settings in cases where conflicts exist with existing serial devices. When using this option enter

the command KVFILE followed by a space, "IRQ", the desired IRQ number, a colon, then the port address (e.g. KVFILE IRQ3:02F8).

Once a linkage to the KEY-VIEW unit is complete, the default modem setup parameters may be modified as shown in Figure 4. Use the keyboard Up Arrow and Down Arrow keys to change between modem setup options. Press the Enter key to toggle between possible setup options, except in the case of the "Init String" and "Alert Call" entries. For the "Init String" line, a valid Hayes Compatible "AT" modem command string should be entered, if necessary. This "AT" command string will be processed after the KEY-VIEW unit processes it's default modem setup command string.

The "Alert Call" line is used to enter an optional pager number that will be called after a possible unauthorized intruder has attempted to access a KEY-VIEW unit causing the unit to automatically lock, as more fully described in section 3.4.5. The first part of the pager number should contain a valid telephone number preceded by any digits needed to obtain access to a phone line (e.g. "9,"). The second portion of the pager number should contain any characters that are necessary to access the paging system. Normally these characters are special modem commands (see your modem reference manual), such as "@" or ",", which cause delays until the paging company is ready to receive data, after the call has been answered. The final part of the pager number must be a numeric code that will clearly indicate to the recipient of the page that a KEY-VIEW unit lock-out has occurred at a particular site (e.g. "911*200" - where the site number is 200). When a pager alert is issued, the KEY-VIEW System automatically adds the applicable unit number that has been locked on to the end of the specified pager dialing string entered, so that this unit number will be transmitted to the pager as the last two digits of the pager code (e.g. 911-200-01). Also, note that when a "*" character is sent to a pager, this character appears as a "-" on the pager display.

If the Alert Call feature of the KEY-VIEW System is not desired, then simply leave the Alert Call entry line blank. Otherwise, after the KEY-

VIEW System has been installed, the Alert Call feature should be tested by sending invalid password(s) to each KEY-VIEW unit to force a lock-out condition to occur and pager calls to be completed.

When all entries have been changed as desired, press the Esc key to exit KVMODEM.EXE processing and save the settings. The new settings will then be transmitted to the KEY-VIEW unit via the serial cable linkage and stored in the KEY-VIEW unit's non-volatile memory.

In order to transfer files from a LOCAL PC to a HOST PC or vice-versa, a program called KVFILE.EXE must be accessible on a disk drive on the HOST PC. KVFILE.EXE processing is initiated by a LOCAL PC to setup the necessary file transfer protocol and serial port interface needed to transfer files between a HOST PC and LOCAL PC. File Transfer procedures using KVFILE.EXE are discussed in detail in section 3.4.7.

The file transfer feature of the KEY-VIEW System is a very useful procedure. For example, assume a Novell Netware file server disk drive fails. Once the network administrator has determined that the drive had failed using KEY-VIEW, the normal procedure would be to initiate Netware's VREPAIR program. However, when the network administrator attempts to initiate VREPAIR, the program file could be missing or corrupt. To remedy this situation, the administrator would use a LOCAL PC to remotely initiate the KVFILE.EXE program on the HOST PC, then transfer a new copy of VREPAIR.EXE to the HOST PC, terminate KVFILE.EXE program execution, then run the newly transferred version of VREPAIR.

Because KVFILE.EXE may need to be invoked on an emergency basis, a second backup copy should also be made of the KVFILE.EXE program to another accessible directory on the HOST PC to help prevent a case where the KVFILE.EXE program becomes damaged or corrupted on the HOST PC.

Once the KVFILE.EXE program has been copied to one or more HOST PC directories, the program and serial linkage between the HOST PC and KEY-VIEW unit can be tested by invoking the program using the command "KVFILE COMx". The "x" in the command indicates the HOST PC's serial port number to which the KEY-VIEW unit is connected and the "x" must be replaced with a number from 1 to 4. If the linkage is successful, a box with the message "KVFILE - READY" appears on the screen. In this case the serial port number to which the KEY-VIEW unit is connected is stored in a file called "KVPORT.DAT, so there is no need to re-specify this port when re-executing the KVFILE.EXE program.

If the COM port number is not specified or is specified incorrectly, the error message "< < COM PORT HAS NOT BEEN SPECIFIED > >" is displayed. If the KEY-VIEW unit is not properly connected to the serial port specified, the message "< < KEY-VIEW NOT FOUND > >" is displayed on the HOST PC. Should this error message occur, it is likely (1) there is a serial port interrupt conflict, (2) the serial cable is not properly connected between the KEY-VIEW unit and HOST PC or is defective, (3) the serial port on the HOST PC has been disabled, or (4) the serial port on the unit and/or HOST PC is defective. Completing a proper serial connection between the HOST PC and KEY-VIEW unit is discussed in section 2.1.0. As a possible step in attempting to resolve the error, try using a different serial port on the HOST PC and/or disable any serial devices on the HOST PC. Then, repeat the test until the linkage can be successfully completed. In some cases a serial port conflict with other devices such as a network card, may exist which causes the HOST PC to lock up after the KVFILE.EXE program is run. As previously mentioned, run the COM911.EXE program provided to help resolve this problem.

In some cases a HOST PC may be automatically set to boot to a specific process that does not permit access to DOS. For example earlier versions of Netware (i.e. version 2.x) and current version of Banyon Vines are normally set to automatically load the network operating system during PC boot processing, in which case the entire hard disk is dedicated to non-DOS partitions. In such cases, these applications should be converted to

boot-up automatically using an AUTOEXEC.BAT file on either a floppy disk drive or hard drive that contains a DOS partition. The beginning of the AUTOEXEC.BAT file should include a command that invokes a special KVWAIT.EXE program, which will cause AUTOEXEC.BAT processing to be terminated if any key is pressed during a specified wait period. The wait period is expressed in seconds as a parameter on the KVWAIT command line. The instructions needed to be placed in an AUTOEXEC.BAT file to accomplish this objective are as follows:

```
KVWAIT 15
REM  KVWAIT sets the DOS Error level to 1 if a key is pressed
REM      within 15 seconds
REM  The Next command causes AUTOEXEC.BAT processing to
REM      skip to :END if a key is pressed
IF ERRORLEVEL==1 GOTO END
..
.. AUTOEXEC.BAT commands needed to start application
..
:END
```

Where necessary, modifying the HOST PC AUTOEXEC.BAT file in this fashion permits a remote user to cold-boot the HOST PC, press a key to terminate normal AUTOEXEC.BAT processing, invoke the KVFILE.EXE program on the HOST PC, and then transfer files between the HOST PC and the LOCAL PC.

2.5.0 KEY-VIEW Configuration Changes

Whenever the video card for a HOST PC is changed or a different cable is used to connect a KEY-VIEW unit to a HOST PC, the KEY-VIEW unit must be re-trained to the new configuration, as described in section 2.2.0.

If the modem connected to a KEY-VIEW unit is changed, then the KVMODEM.EXE program may need to be used to set the modem parameters for the new modem, as previously discussed.

If a different KEY-VIEW unit is installed as unit ID 00 and other than the default modem string is necessary for the KEY-VIEW unit to properly initialize the modem connected to the KEY-VIEW unit, the KVMODEM.EXE program must be re-run to setup the new KEY-VIEW unit for the desired modem settings.

After any changes are made to the KEY-VIEW System configuration, all users who may need to access the unit(s) should re-test to confirm that access is possible after the changes are made.

At this point the installation of the KEY-VIEW unit on the HOST PC is complete. The next steps in the installation process involve installing KEY-VIEW software on each LOCAL PC that will be used to access the HOST PC and testing the linkage between each LOCAL PC and each KEY-VIEW unit to be accessed.

3.0.0 KEY-VIEW LOCAL PC PROCEDURES

KEY-VIEW software must be installed on each LOCAL PC used to access one or more KEY-VIEW units. There are no additional license fees for installing the software on multiple LOCAL PC's. Each LOCAL PC must have an internal or external Hayes compatible modem. As previously discussed, it is strongly suggested that all LOCAL PC's use one of recommended modems listed in the README.TXT file.

To install KEY-VIEW software on a LOCAL PC: (1) use the DOS MD command to make a directory on the LOCAL PC's disk drive, such as "KEYVIEW" or "KV" and (2) copy the contents KEY-VIEW Installation diskette's root directory to the directory created on the LOCAL PC. There is no need to copy the contents of the HOST directory to a LOCAL PC. The files contained in the HOST directory need only be installed on HOST PCs as discussed in section 2.4.0.

Important: *Before initiating the KEYVIEW.BAT program on the LOCAL PC make sure any Terminate and Stay Resident (TSR) programs; such as Microsoft Windows, Borland's Sidekick, Norton's DOS line editor, etc. that may scan keyboard input looking for "Hot Keys" or the "EXIT" command; are not placed in memory during the boot initialization process, or are removed from memory. Such programs attempt to take over or control the LOCAL PC's keyboard and could cause the PC to lockup or KEY-VIEW System processing to fail.*

After the KEY-VIEW software has been copied on to a LOCAL PC, a linkage to a KEY-VIEW unit can be initiated by running the KEYVIEW.BAT program from the LOCAL PC's directory where the KEY-VIEW software was installed. When KEYVIEW.BAT processing is initiated, an animated demonstration begins illustrating KEY-VIEW's capabilities. This demonstration lasts for approximately 30 seconds and can be aborted at any time by pressing any key.

After the animated demonstration has ended, the Main Menu screen is displayed as shown in Figure 5. The box on the right hand section of the screen shows the "Connection Status" of any active linkage between the LOCAL PC and a KEY-VIEW unit. When the LOCAL PC is remotely linked to a KEY-VIEW unit, the unit's two digit ID, description, display mode, and lock-out limits are displayed in this box. Possible display mode settings are discussed in section 3.4.1 below. Lock-out limits are discussed in section 3.4.5. Also, the "Connection Status" box indicates if the LOCAL PC has been set to either a "HOST" mode or a "LOCAL" mode, as described in section 3.4.2. Figure 13 illustrates the contents of the "Connection Status" box after a connection to a KEY-VIEW unit has been completed.

Some users may wish to access a HOST PC by using Palmtops or other devices where disk storage may be limited in the LOCAL PC. In such cases, only the KVLINK.EXE and USER.DAT (if present) files need be copied to the LOCAL PC to permit access to a HOST PC. These files require less than 70K of storage space. After these files are copied, execute the KVLINK.EXE program to begin an access session instead of using the KEYVIEW.BAT program. The only difference between initiating an access session using KVLINK.EXE and KEYVIEW.BAT is that the animated demonstration will be skipped.

3.1.0 KEY-VIEW Overview

When the KEYVIEW.BAT program is run for the first time, the "Setup KEY-VIEW" main menu option must be selected to setup (1) the "Call List" of KEY-VIEW units that may be accessed by the LOCAL PC and (2) the "Modem Setup" specifications needed to initialize and access the modem connected to the LOCAL PC.

Once the initial "Setup" process for a PC has been completed, the contents of that LOCAL PC's KEY-VIEW directory may be copied to other LOCAL PC's and modified as necessary to avoid having to re-create duplicate call lists.

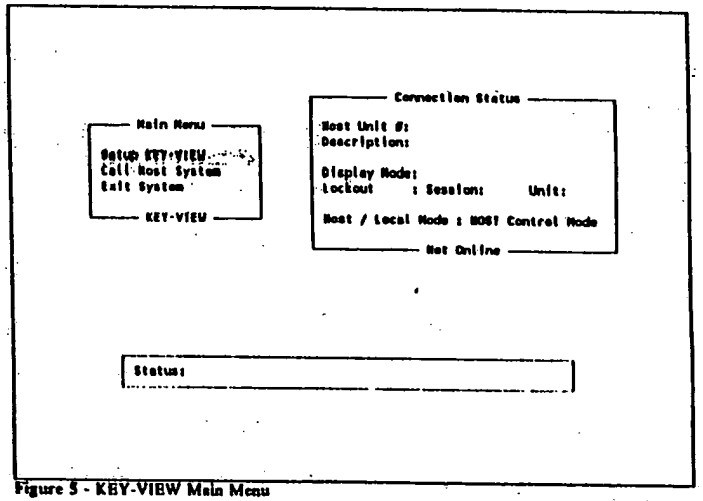

Figure 5 - KEY-VIEW Main Menu

As mentioned when KEYVIEW.BAT processing ends, a Main Menu of processing options is displayed as shown in Figure 5. A description of the processing occurring under each of these options is described next.

3.2.0 Setup KEY-VIEW Processing Options

This Main Menu option displays a menu of KEY-VIEW "Setup" processing options as shown in Figure 6. A detailed description of the processing occurring under each of these menu options is as follows:

3.2.1 Call List Processing

This menu option allows each KEY-VIEW unit that a LOCAL PC may access to be defined, as shown in Figure 7. Before a call can be placed to KEY-VIEW unit, the unit must be defined as a line item in this call list.

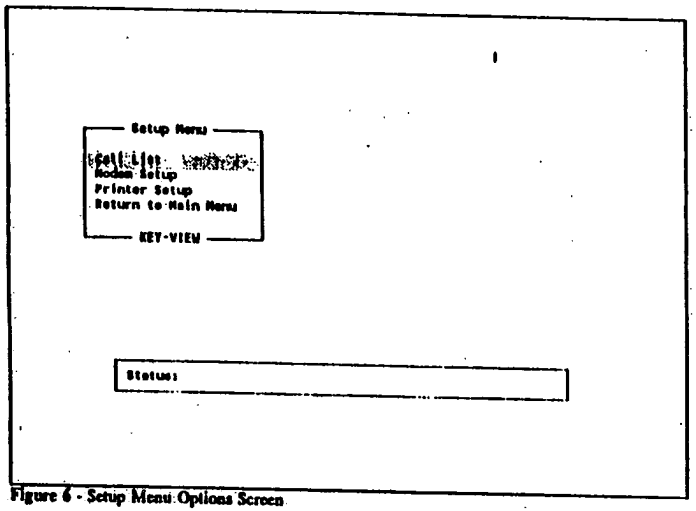

Figure 6 - Setup Menu Options Screen

The specific data elements that must be entered for each KEY-VIEW unit to be accessed are as follows:

- LOCATION DESCRIPTION - This is a user definable, 20 character alphanumeric description of the HOST PC unit being accessed such as "SERVER XYZ", "BACKUP TAPE UNIT", etc. Entering clear descriptions helps users with access to multiple HOST PCs more easily select the desired KEY-VIEW unit.

- DIALING STRING - This field may contain up to a 30 character dialing string needed to access the modem at the site where the HOST PC(s) is located. Numerics and modem compatible special characters; such as "," or "@" characters; may be entered as part of the dialing string. Consult the reference manual supplied with the

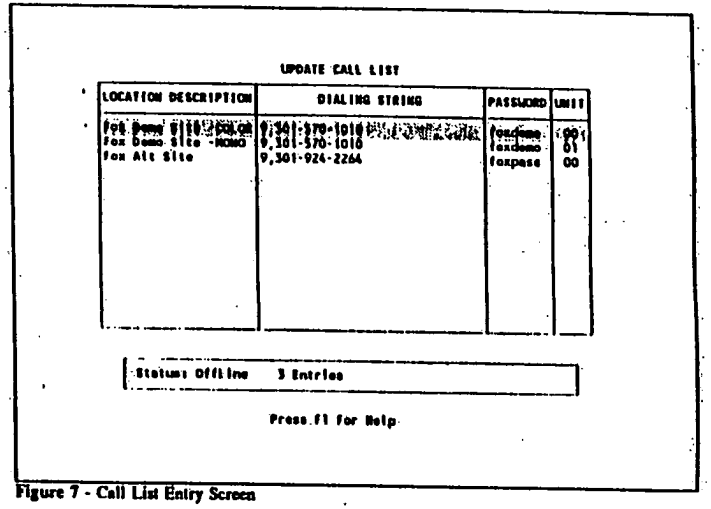

Figure 7 - Call List Entry Screen

modem to determine the effect of any special characters included in a dialing string. When a KEY-VIEW unit is being accessed in a "Direct Connect" mode, as more fully described in section 3.2.2; a dialing string should not be specified.

- PASSWORD - This field must contain an alphanumeric password, no longer than 8 digits, that will be used to control access to the KEY-VIEW unit and the HOST PC. All alphabetic characters entered for a password are case sensitive. In other words, if the password defined is "Ball", using "BALL" or "ball" as a password would not permit access to the KEY-VIEW unit. The password entered must be the currently active password for a KEY-VIEW unit. A KEY-VIEW unit password can only be changed after the KEY-VIEW unit has been successfully accessed from a LOCAL PC,

as discussed later in this section. If a password for a KEY-VIEW unit is lost, the unit will not be accessible unless the unit is returned to Fox Network Systems to restore the password to it's default setting, which involves shipping expenses and a handling fee. Accordingly, always retain a central, current list of the passwords assigned to KEY-VIEW units.

When a KEY-VIEW unit is first installed, the default password is "KEYVIEW". This password must be entered using only capital letters and must be used to initially access the KEY-VIEW unit. After accessing the unit for the first time, it is suggested that this password be changed to a new password as described in section 3.4.5.

- UNIT - the unit ID entered in this field must be between 00 and 59 and correspond to the KEY-VIEW unit DIP switch settings located on the left rear side of the KEY-VIEW unit to be accessed. DIP switch settings represent binary values reading from left to right. On this basis, if only the left most DIP switch is set to the UP position, the unit ID would be 1. If the left most two DIPs switches were set to the UP position, the unit ID would be 3, (i.e. 1+2) and so forth. Appendix A contains the a complete list of the decimal value (i.e unit ID) for all possible combinations of DIP switch settings. In order to remotely access a KEY-VIEW unit, the unit ID must be correctly defined on the LOCAL PC's call list. **KEY-VIEW units may not be accessible remotely if any unit IDs on a daisy-chain are not unique, the unit connected to the modem is not set to unit ID 00, or an incorrect unit ID is specified in the call list!**

New call list entries should be added using the Down Arrow key to go to the last line of the call list which will be a blank line. Then, fill in the blank line with the data for the new unit.

An entry may be flagged for deletion from the call list by using the Up Arrow or Down Arrow keys to highlight the applicable line item and then

pressing the Ctrl/Delete keys. Other keys used to navigate through the call list can be viewed by pressing the F1 help key. Figure 8 contains the pop-up help screen that appears when the F1 key is pressed. Press the Esc key to exit from this help menu.

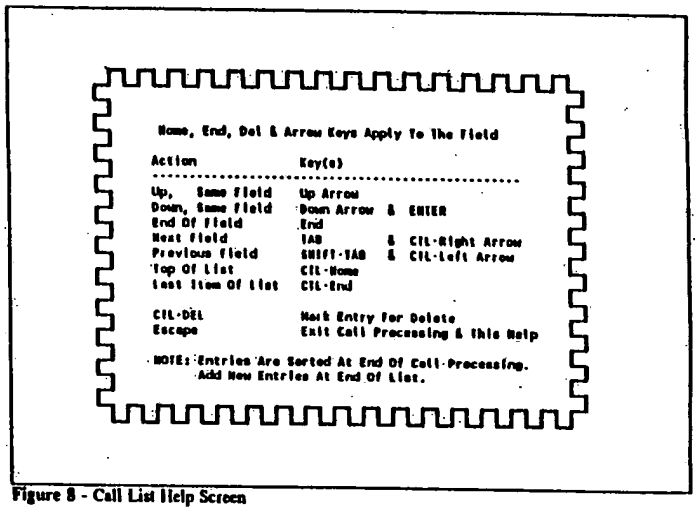

Figure 8 - Call List Help Screen

A call list entry may be changed by highlighting the applicable line item, then changing the data contained on the line, as desired.

Once all required modifications have been made to the call list, press the Esc key to return to the Setup Menu. When the Esc key is pressed, any changes made to the call list are saved to a USER.DAT configuration file on the LOCAL PC's disk drive.

3.2.2 *Modem Setup*

The "Modem Setup" menu option allows the serial port number, baud rate and reset string to be defined for the modem connected to the LOCAL PC or to permit a KEY-VIEW unit to be directly connected (via a dedicated RJ-45 cable) to a LOCAL PC's serial port, in which case no modems are necessary for either the LOCAL PC or the HOST site.

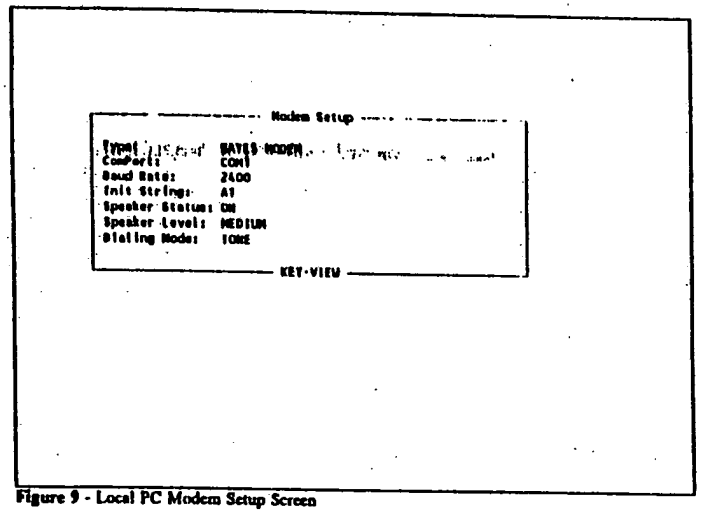

Figure 9 - Local PC Modem Setup Screen

When the "Modem Setup" option is selected, a screen appears as illustrated in Figure 9. The first entry on the screen permits changing the LOCAL PC to either a "Direct Connect" or "HAYES MODEM" mode. When the cursor is positioned on this entry, the mode can be changed by pressing the Enter key.

The "Direct Connect" mode should only be selected when a KEY-VIEW unit is directly connected (via a dedicated RJ-45 cable and an optional Direct Connect serial port adapter) to one of the LOCAL PC's serial ports. In this case, only the "ComPort" and "Baud Rate" data entry items need to be defined for direct connection. Also, the KEY-VIEW unit's ID to which the LOCAL PC is connected should be other than unit ID 00. If the "HAYES MODEM" option is selected, all data entry items requested on the screen should be completed.

Once the desired mode has been selected, press the Down Arrow or Up Arrow keys to change to the next data entry item. The Esc key may be pressed at any time to save all settings displayed on the screen to a USER.DAT configuration file on the LOCAL PC's disk drive, after which processing returns to the Setup Menu.

The "ComPort" data entry item permits defining the serial port number of the LOCAL PC that will be used by the KEY-VIEW software to communicate with a KEY-VIEW unit. A utility program (COM911.EXE) on the KEY-VIEW installation diskette may be run to determine the serial port to which the modem is connected. The serial port number specified is normally a number between 1 to 4. To change to a different serial port number, simply press the Enter key until the desired serial port number is shown. When the "Other" option appears as the "ComPort", advanced users may specify the actual IRQ and Address to be used for access to the LOCAL PC's modem in various pop-up windows. In this case, use the Tab and Enter keys to modify the "Other" port specifications, as instructed on screen, then press the Esc key to exit from the pop-up windows after the desired setting have been entered. After the serial port has been specified, either press the Down Arrow or Up Arrow key to move to another item or press the Esc key to save all settings displayed on the screen.

The "Baud Rate" data entry item permits defining the speed at which the LOCAL PC will transfer data to and from the KEY-VIEW unit. Baud rates may be changed using the Down Arrow or Up Arrow keys to

position the cursor on this data entry item. Then, press the Enter key until the desired baud rate appears.

The default "Init String" is used to initialize the LOCAL PC's modem immediately prior to placing a call to a KEY-VIEW unit. The default string is normally used for most HAYES compatible modems and must begin with "AT". This reset string may need to be modified in certain cases. Any known suggested modifications for particular brands of modems are included in the README.TXT file. If one of the listed modems in the README.TXT file is being used by the LOCAL PC, then modify the default reset string to the appropriate string listed in the README.TXT file. This string will be ignored in cases where the LOCAL PC is in a "Direct Connect" mode.

The "Speaker Status" permits the LOCAL PC modem's speaker to be turned "ON" or "OFF". Assuming the LOCAL PC's modem is equipped with an operable speaker, when the "Speaker Status" is set to "ON", the LOCAL user will be able to monitor the sounds emitted from the phone line during the initial linkage to the HOST sites modem. After the connection is completed, the speaker will be turned off automatically. If the "Speaker Status" is set to "OFF", the modem speaker will be disabled, thereby preventing the LOCAL user from monitoring the progress of the phone call. It is suggested that the "Speaker Status" be set to "ON", so that situations where line noise exists during a call can be detected.

The "Speaker Level" permits setting the speaker volume level to either "HIGH", "MEDIUM", or "LOW". It is suggested that the "MEDIUM" setting be selected.

The "Dialing Mode" permits selecting either a touch "TONE" or "PULSE" mode. Almost all phone systems use the "TONE" mode, which is the recommended choice.

Once all data items have been set to their desired values, press the Esc key to save the information to disk and return to the Setup Menu.

3.2.3 Printer Setup

When connected to a HOST PC, the KEY-VIEW System permits the HOST PC's screen contents to be sent to a file or printer connected to the LOCAL PC's default printer port, similar to the Print Screen key on a PC keyboard. This print screen feature only works with text modes and text based printers and will not work, for example, with printers set to a postscript mode. As illustrated in Figure 10, the "Printer Setup" menu selection permits changes to the options available to print a screen, as follows:

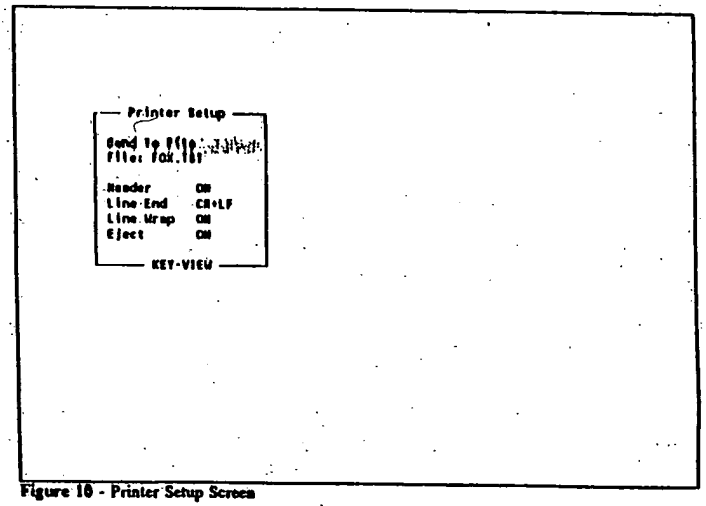

Figure 10 - Printer Setup Screen

- SEND TO FILE/PRINTER - This field determines if the screen contents are to be sent directly to the Printer (i.e. "Send to Printer") or to a data file (i.e. "Send to File"). Toggling between these two options can be accomplished by pressing the Enter key, after using

the Up Arrow or Down Arrow key to highlight this field.

- FILE - Enter the file name where screen data will be sent if the "Send to File" print option has been selected. This file name is ignored when the "Send to Print" option has been selected. The file name is limited to 13 characters. The file contents will be stored in the KEY-VIEW default directory unless another drive and/or directory is specified. If the specified file is present at the time a new screen is saved, print screen data sent to this file will be appended to the end of the file. If the saved print screen data in a file is no longer needed, delete the file and the KEY-VIEW System will simply create a new file the next time screen data is saved to the file. During an access session, the file name may be changed as often as necessary so that screens may be saved to different file names.

- HEADER - When "ON", a heading banner is printed before printing the contents of the HOST PC screen. This banner shows the KEY-VIEW unit's description and number (from the Call List) and the time and date the print out occurred. When" OFF" the heading section is not printed before each screen printed. Toggling between the "ON" and "OFF" options can be accomplished by pressing the Enter key.

- LINE END - When each line of screen data is sent to the printer, the printer may require special carriage return (CR) and line feed (LF) characters to skip to the next line. Most printers require both a CR + LF, so normally the "Line End" option is selected. If this option does not work properly for a particular printer, press the Enter key to select another available option, then test if the new option corrects the problem.

- LINE WRAP - Some printers require an end of line code to tell the printer to begin a new line. In such cases without this special code only the first line of screen data will print. This code will be

inserted at the end of each print line sent to the printer when this option is "ON". If this option is set to "OFF", no end of line code will be sent to the printer. Normally, this option is set to "ON". Toggling between the "ON" and "OFF" options can be accomplished by pressing the Enter key.

- EJECT - If this option is "ON", a page eject command will be sent to the printer after a screen is printed. Otherwise, no eject command will be sent. If this option is set to "OFF", some screen printouts may overlap pages, because no ejects will be issued. In any event, prior to printing the first screen, the printer should be set to the top of a page, since no ejects are issued before a screen is printed. Toggling between the "ON" and "OFF" options can be accomplished by pressing the Enter key.

  When EJECT is set to "OFF", the KEY-VIEW Main Menu (see Figure 13) automatically contains an additional menu option called "Printer Eject". When this option is selected, a printer page eject command is send to either the default printer or specified print file.

3.2.4 Return to Main Menu

When "Return to Main is selected from the Setup Menu, processing returns to the KEY-VIEW Main Menu.

3.3.0 Calling A KEY-VIEW HOST Unit

When selected, the "Call Host System" Main Menu option (see Figure 5) displays the latest call list of KEY-VIEW units that may be accessed by the LOCAL PC as shown in Figure 11. This call table was setup as previously discussed in section 3.2.1 above.

If there are no entries on the call list, an error message is displayed indicating the call list must be setup before attempting to access an installed KEY-VIEW unit. Then, processing is returned to the KEY-VIEW

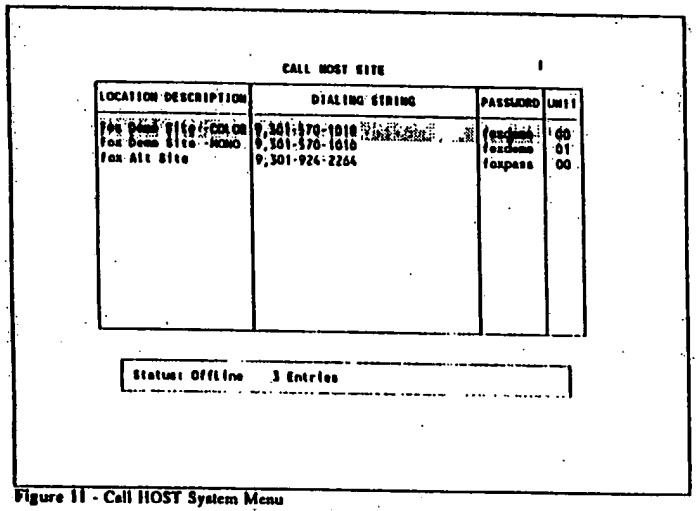

Figure 11 - Call HOST System Menu

Main Menu. Otherwise, the list of KEY-VIEW units is displayed permitting selection of the desired unit to be accessed. If access is not desired to any of the listed units, the **Esc** key may be pressed to end call list processing and return to the KEY-VIEW Main Menu.

Only a maximum of 13 KEY-VIEW unit descriptions appear on the screen at a time. If more than 13 units exist on the call list, the **Up Arrow**, **Down Arrow**, **Page Up**, or **Page Down** keys can be used to scroll through the entire list of KEY-VIEW units defined. Once the desired KEY-VIEW unit has been highlighted, press the **Enter** key to initiate HOST PC access processing.

When HOST PC access processing is initiated, the dialing string for the selected call list entry is used to initiate a call from the LOCAL PC's modem to the HOST site's modem (or the KEY-VIEW unit is accessed

directly through the LOCAL PC's serial port in the case where a "Direct Connect" mode has been specified.)

When a call is initiated using a modem, it may take as long as 30 seconds to initialize the modem and complete the connection to a KEY-VIEW unit at the HOST site. During this process, the "Status:" block on the LOCAL PC's screen will indicate what steps are occurring. These status messages typically include (1) "Dialing HOST", (2) "Please Wait ...", (3) "Connect 2400", (4) "Accessing Unit", (5) "Sending Password" and (6) "Checking Security".

During the initial linkage to a HOST site, a large portion of time spent results from security precautions taken. For example, the password sent is highly encrypted, so that even if someone were monitoring the call, the password would be virtually impossible to detect, decode or copy. In cases where telephone line noise or static is present during initial access to a KEY-VIEW unit, a valid password may be garbled and rejected by the unit. In such cases, the phone line connection to the HOST site should be terminated and the site called again, which normally clears up any telephone line noise.

Once the linkage to a HOST site is successfully accomplished, the user is connected to the applicable KEY-VIEW unit ID specified in the call list and automatically logged into the KEY-VIEW unit using the password from the call table. If the LOCAL PC's modem cannot establish a connection to the HOST site's modem; the LOCAL PC's modem is reset, the phone line is put on-hook and processing returns to the KEY-VIEW Main Menu.

If the LOCAL PC's modem connects to the HOST site's modem, but the requested KEY-VIEW unit ID does not exist; the desired KEY-VIEW unit does not respond to the access request; or the password specified is incorrect, an appropriate error message is displayed on the LOCAL PC's screen, the LOCAL PC remains connected to the HOST site modem and the KEY-VIEW Main Menu appears as illustrated in Figure 13.

Normally, the background behind the pop up window shows the status of the Host PC's video display (in text modes only). However, in this case, the background behind the pop up Main Menu will be blank, because no connection to a KEY-VIEW unit is currently active. Since the LOCAL PC is not actually connected to a KEY-VIEW unit, the "Connection Options" menu displays only four options, namely "Switch Host/Local Mode", "Switch Units", "Terminate Connection", or "Return to Main Menu".

In cases where (1) a LOCAL PC links with a HOST site modem, but an initial connection to a specified KEY-VIEW unit cannot be completed, (2) a linkage cannot be established to another KEY-VIEW unit by using the "Switch Units" connection option; or (3) an active linkage to a KEY-VIEW unit is dropped (possibly due to phone line interference) but the modem linkage continues; the LOCAL PC will remain connected to the HOST, as previously discussed.

When any one of these situations occur, several actions may be taken. First, if an incorrect password or unit ID was specified for access to the selected KEY-VIEW unit, the "Setup KEY-VIEW" menu option could be selected, the "Call List" menu option selected, and the password and/or unit ID for the selected unit changed, as discussed in section 3.2.1. Then, the "Connection Options" could be selected from the Main Menu, the "Switch Units" menu option selected and the desired unit could be re-selected from the call list. Second, if the password is correct, a connection may be re-established simply by re-selecting the KEY-VIEW unit from the "Switch Unit" call list. In this case, telephone line noise or static may be preventing the KEY-VIEW unit from receiving the correct password. If repeated attempts to access the KEY-VIEW unit fail, then terminate the connection from the "Connection Options" menu, wait about 1 minute for the unit(s) at the HOST site to reset, which is done automatically whenever the phone connection is lost, then re-call the site and attempt to access the selected unit. If the KEY-VIEW unit is still inaccessible, either the password specified is incorrect, the unit has failed or has been turned OFF, the cabling to the unit is not properly connected, or the unit has been locked due to unauthorized security access breaches (see section 3.4.5).

The final option that can be taken, when a unit connection can't be completed or is lost, is to terminate the connection from the "Connection Options" menu and retry calling the site again, as previously discussed.

In some cases, the message "No Video Signal Present" may appear after a KEY-VIEW unit has been successfully accessed. When this message appears the KEY-VIEW screen will be blank. This message means that no electrical signals are being received from the HOST PC video display adapter card. This situation will occur if (1) the cable between the KEY-VIEW unit and HOST PC's video display adapter card has been disconnected, (2) the HOST PC's video adapter card has failed completely, or (3) the HOST PC has been turned OFF, failed or lost power.

When a KEY-VIEW unit is first accessed, it beeps three times to alert personnel that a remote user is attempting to access the KEY-VIEW unit. If the unit lock-out counter has reached it's limit (see section 3.4.5), a message appears in the "Status" box indicating that the "Unit Is Locked Out", and no further access is permitted. In this case someone at the HOST site must press the "ACTION" button on the front of the locked KEY-VIEW unit in order to permit access to the unit. When such lockouts occur and cannot be explained, it is suggested that the phone number used to access the HOST site be changed to a new phone number.

If the KEY-VIEW unit is not locked, the password sent from the LOCAL PC is un-encrypted and validated by the KEY-VIEW unit. Each time a password is validated, both the LOCAL PC and KEY-VIEW unit emit a short beep tone. If a password received is invalid, the KEY-VIEW unit automatically requests the LOCAL PC to re-transmit the password to ensure that transmission problems did not affect the validity of the password. A short beep tone will precede each such attempt. If after several attempts, the password is still invalid, the message "Invalid Password" appears in the Status box on the LOCAL PC monitor screen, and further access to the KEY-VIEW unit is denied. At this point the remote user may be locked out of the KEY-VIEW unit for the session or

until someone presses the "ACTION" button on the front of the KEY-VIEW unit, as more fully described in section 3.4.5.

Immediately after a valid password is received, the KEY-VIEW unit checks it's internally maintained unit lock-out counter. As described more fully in section 3.4.5, this counter indicates if unsuccessful attempts have been made to access the KEY-VIEW unit that would be indicative of an intruder trying to guess the unit's password. If the unit lock-out counter is not equal to zero, a warning message appears in the "Status" box on the LOCAL PC screen indicating the number of concurrent prior sessions where unauthorized attempts were detected (i.e. since the last successful access to the unit had occurred). Then, the lock-out counter is then reset to zero. This approach ensures an authorized user is made aware of possible recent attempted security violations.

After a valid password is received and security processing has been completed, a "Connect Options" menu is displayed as shown in Figure 12. The first option, "Direct Access" provides both keyboard and video screen access to a HOST PC. The second option, "View Host Only" provides access only to the HOST PC's video screen. In this case no access is provided to a HOST PC's keyboard. The option selected remains in effect until the access to the KEY-VIEW unit is terminated. To change to a different Connect Option without terminating the telephone connection to a HOST site, simply select the "Switch Units" option (see section 3.4.4), then re-select the same HOST PC, which causes the Connect Options menu to re-appear for that HOST PC.

Once one of these options is selected, the HOST PC screen contents will appear on the LOCAL PC's screen. At this point processing may be temporarily returned to the KEY-VIEW Main Menu by pressing the Left Shift key three times in rapid succession.

Whenever a LOCAL PC is connected to a HOST site and the Left Shift key is used to pop-up the KEY-VIEW Main Menu, information related to the active HOST PC connection is displayed on the right hand section of

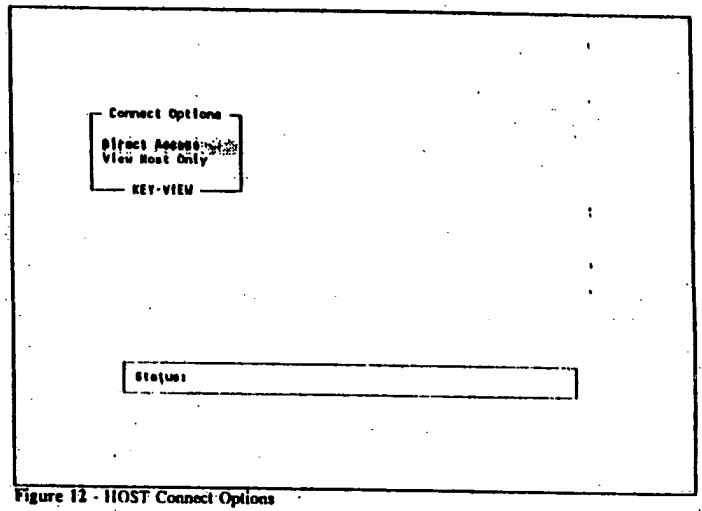

Figure 12 - HOST Connect Options

the KEY-VIEW Main Menu (see Figure 13) and data from the HOST PC screen appears behind KEY-VIEW's pop-up windows, except when the HOST PC's screen is in a graphics mode. The pop-up windows can be removed from the screen by selecting the "Exit to HOST" menu option from the Main Menu or by pressing the Esc key. Also, notice that the second selection on the KEY-VIEW Main Menu (see Figure 5) is changed from "Call HOST System" to "Connection Options".

When EJECT is set to "OFF", as discussed in section 3.2.3, the KEY-VIEW Main Menu (see Figure 13) automatically contains an additional menu option called "Printer Eject". When this option is selected, a printer page eject command is send to either the designated printer or print file.

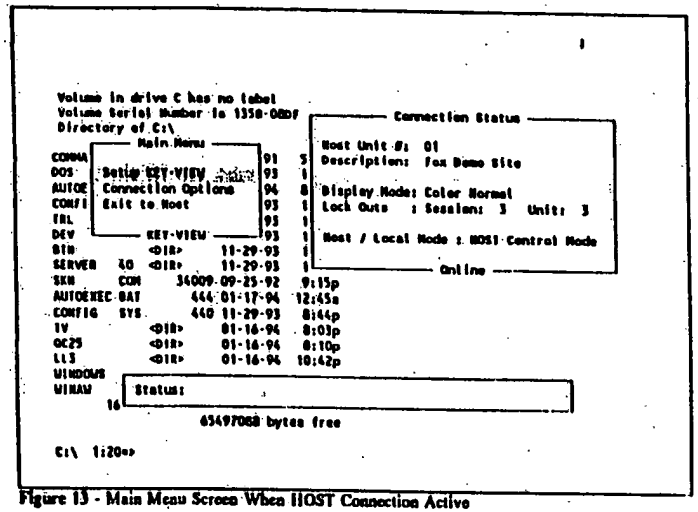

Figure 13 - Main Menu Screen When HOST Connection Active

3.4.0 KEY-VIEW Connection Options

"Connection Options" appears on the KEY-VIEW Main Menu only when a connection is active to a HOST site. When selected, a menu of connection processing options is displayed as shown in Figure 14. As mentioned in section 3.3.0, not all connection options may be available for use, if, for example, a connection to a particular KEY-VIEW unit cannot be completed. A detailed description of the processing occurring under each of the possible Connection Menu options follows.

3.4.1 Set Display Mode

In cases where a KEY-VIEW unit is connected to a HOST PC with a non-VGA video card (i.e. a card having a 9 pin video output connector), data will be displayed on the LOCAL PC in a monochrome mode. In this case,

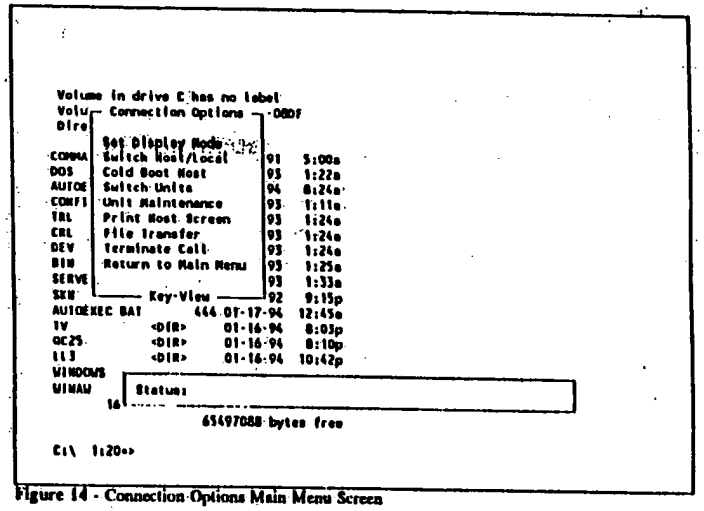

Figure 14 - Connection Options Main Menu Screen

the "Set Display Mode" option will normally not appear and this section should be ignored. If the menu option should appear, it is recommended that only the default "Mono Green" be selected, as shown in Figure 15. In either case the remainder of this section should be ignored for non-VGA HOST PC installations.

When a KEY-VIEW unit is connected to a HOST PC with a VGA display card, the video output consists of three primary color signals, namely green, red, and blue. The "Set Display Mode" menu option permits a LOCAL PC to view VGA text video output of a HOST PC in either a color or monochrome mode. VGA graphics can presently be viewed only in a monochrome mode and is unaffected by video display mode changes discussed in this section. When exiting from a graphics mode to a text mode on a HOST PC, the Left Ctrl key on the LOCAL PC must be

pressed rapidly three times to cause the KEY-VIEW unit to switch to a text mode. If this procedure is not followed, the LOCAL PC's screen will appear blank or freeze until the **Left Ctrl** key is pressed, as described.

If a color mode is selected, text data may be viewed in color in either a high or normal intensity. The only difference between these two choices is in brightness of the colors displayed. Data transfer speeds will be identical in either case. However, when either of these color mode options are selected screen transfer rates will be about 50% slower than selecting one of the three monochrome mode options. In addition, the cursor may not appear when a color mode is selected, due to the processing delays required to decode color information.

In almost all cases, the colors displayed on a LOCAL PC will be the same as the colors displayed on a HOST PC. The monitor actually connected to a HOST PC has no impact on the KEY-VIEW System's ability to display data on a LOCAL PC in color (assuming the LOCAL PC has a color monitor). In other words, in cases where a HOST PC has a VGA monochrome monitor or no VGA monitor attached, video output of a HOST PC can still be displayed on a LOCAL PC in color.

In some cases, it is possible the KEY-VIEW unit may not be able to decode the HOST PC VGA text data. This would only occur when an application displays text data using the same foreground and background color with varying intensities, such as pink on red, grey on black, etc. Since such color combinations are nearly impossible for users to read, most applications naturally avoid such color combinations. As a result, it would be rare for a KEY-VIEW unit to be unable to decode text data. Some applications, such as CMOS setup screens, use unusual color combinations that can only be effectively displayed by selecting one of the two color display modes.

When displaying VGA output in monochrome, it is possible to select any one of the three primary color signals for display purposes. Normally, selecting the green signal yields the best monochrome results. If none of

the three monochrome options produce a satisfactory screen, then selecting one of the two color mode options normally yields satisfactory results.

The last "Set Display Mode" option forces the KEY-VIEW unit to display the contents of the HOST PC's screen in a "Graphic Snapshot" format. In this case, whatever information will be presently displayed on the HOST PC's screen in either text or graphics mode is displayed on the LOCAL PC's screen in a graphics mode. If the HOST PC is in a text mode, the text data will appear reduced in size on the LOCAL PC, when the Graphic Snapshot option is selected. New "Graphic Snapshots" of the latest screen displayed on the HOST PC will be taken each time the **Right Shift** key is pressed twice in rapid succession. To exit out of a "Graphics Snapshot" mode, press the **Left Shift** key three times in rapid succession to pop-up the KEY-VIEW menus; then select another video display mode option. If a HOST screen is in a graphics mode, all video display options will be ignored until the HOST PC is placed in a non-graphics mode. The 640x480 VGA graphics mode is presently the only graphics mode fully supported by the KEY-VIEW System.

When "Set Display Mode" option is selected, a menu of the six possible display modes appears as shown in Figure 15. The **Up Arrow** and **Down Arrow** keys can be used to change between display modes. Then, press the **Enter** key to select a specific mode. For text based applications, the "Mono Green" mode is normally selected as the default mode.

3.4.2 Switch HOST/LOCAL Mode

This menu item sets the options that are available when exiting from the KEY-VIEW Main Menu. Two possible modes appear when the "Switch HOST/LOCAL" option is selected, as shown in Figure 16. Select the desired option using the **Up Arrow** and **Down Arrow** keys and then press the **Enter** key.

If the "Local PC Mode" option is selected, the last menu option on the KEY-VIEW Main Menu will be changed from "Exit to HOST" to "Exit to DOS". This option then permits "shelling-out" of the KEY-VIEW

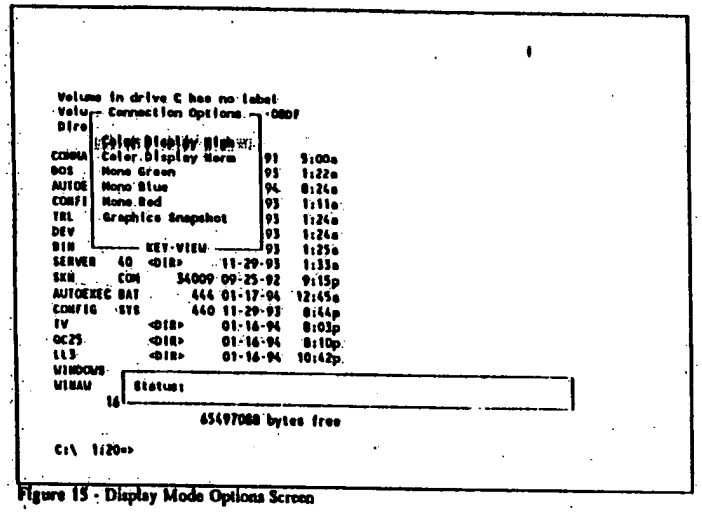

Figure 15 - Display Mode Options Screen

application to DOS on the LOCAL PC while continuing to maintain a connection to the HOST site. When shelling-out to DOS in this manner, the KEY-VIEW System remains resident and takes about 100K of the LOCAL PC's memory. Once DOS processing has been completed, a user may then return to the KEY-VIEW Main Menu by typing "EXIT" at a DOS prompt.

If the "Host Control Mode" menu option is selected, the last menu option on the KEY-VIEW Main Menu will be "Exit to HOST". When the "Exit to HOST" option is selected, the LOCAL PC's video monitor displays the screen contents of the HOST PC, and the LOCAL PC's keyboard is re-directed to control the HOST PC. In this case, processing could be returned to the KEY-VIEW Main Menu by pressing the Left Shift key three times in rapid succession. The default mode is the Host Control Mode.

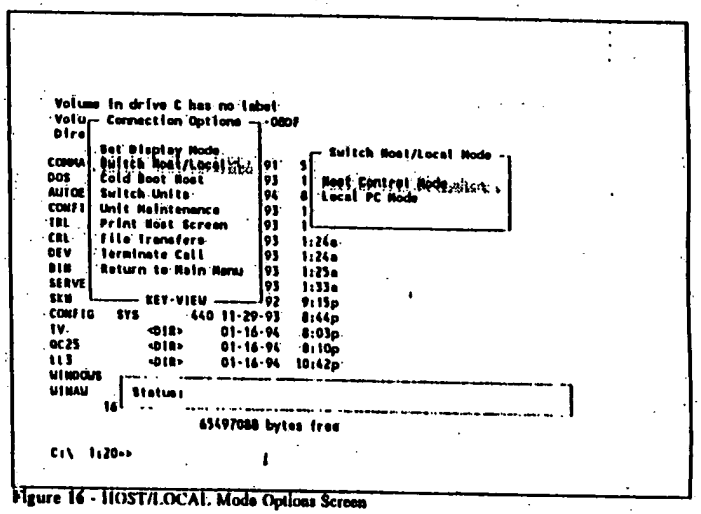

Figure 16 - HOST/LOCAL Mode Options Screen

After the HOST or LOCAL option is selected from the menu or the Esc key is pressed, processing is returned to the Connections Options menu.

3.4.3 Cold Boot Host

When this Connection Option is selected, the cold-boot request must be confirmed by entering "Y" in response to the question "ARE YOU SURE? (Y/N)" (see Figure 17). If "N" is entered or the Esc key is pressed in response to the question, cold-boot processing is aborted and processing returns to the Connections Options menu. If "Y" is entered, the LOCAL PC sends instructions to the KEY-VIEW unit to temporarily interrupt AC power to the HOST PC for approximately 15 seconds. Once power is restored to the HOST PC, the KEY-VIEW unit returns a confirmation to the LOCAL PC that power has been restored to the HOST PC, which is displayed briefly in the Status box on the LOCAL PC. Then, processing

automatically returns to the HOST PC's screen so that the LOCAL PC can view the reboot process.

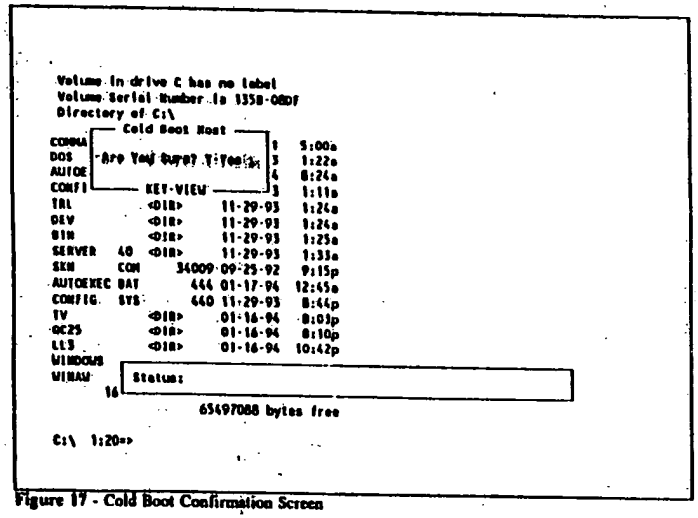

Figure 17 - Cold Boot Confirmation Screen

It is also possible to warm boot a HOST PC from a LOCAL PC, but it is suggested that the cold boot option be used instead. Warm booting can be accomplished by first selecting "HOST Control mode" from the KEY-VIEW Main Menu. When in the "HOST Control mode", the LOCAL PC takes over the HOST PC's keyboard. So, when the Ctrl, Alt, and Delete keys are pressed at the same time, the HOST PC will be warm booted. During this boot process, the LOCAL PC will remain connected to the HOST PC, so that the reboot process may be monitored and controlled by the LOCAL PC. As is the case with warm booting any PC, a warm boot may not achieve it's desired result if the HOST PC's processor is locked

up, or the keyboard is frozen. In this case the HOST PC must be cold-booted, as described above, to unlock the HOST PC's processor.

3.4.4 Switch Units

This menu option permits switching between KEY-VIEW units that are daisy-chained together at a HOST site. If only one KEY-VIEW unit is accessible at the HOST site, there would normally be no reason to select this menu option. In cases where it is desired to switch from one KEY-VIEW unit to another KEY-VIEW unit accessible through a different modem (i.e. at another site), the connection to the current site must be terminated by selecting the "Terminate Call" menu option. Then, a connection must be established to the new site, as more fully described in section 3.3.0.

As shown in Figure 18, when the "Switch Units" option is selected, the call list contains only those KEY-VIEW units that have the exact same phone dialing string. Units using the same dialing string are assumed to be daisy-chained together at a HOST site.

This list of KEY-VIEW units is displayed to permit switching between KEY-VIEW units which are daisy-chained together, without the need to terminate the existing phone line connection. The Esc key may be pressed to avoid switching to another unit after the "Switch Units" menu option is selected. The F1 key may be pressed to pop-up a Help screen related to Call List processing (see Figure 18).

Only a maximum of 13 KEY-VIEW unit descriptions appear on a screen at a time. If more than 13 units have been daisy-chained together and exist on the call list, the Up Arrow, Down Arrow, Page Up or Page Down keys can be used to scroll through the entire list of KEY-VIEW units defined. Once the desired KEY-VIEW unit has been highlighted, press the Enter key to switch to that KEY-VIEW unit.

If the new KEY-VIEW unit is inaccessible or the password used for the

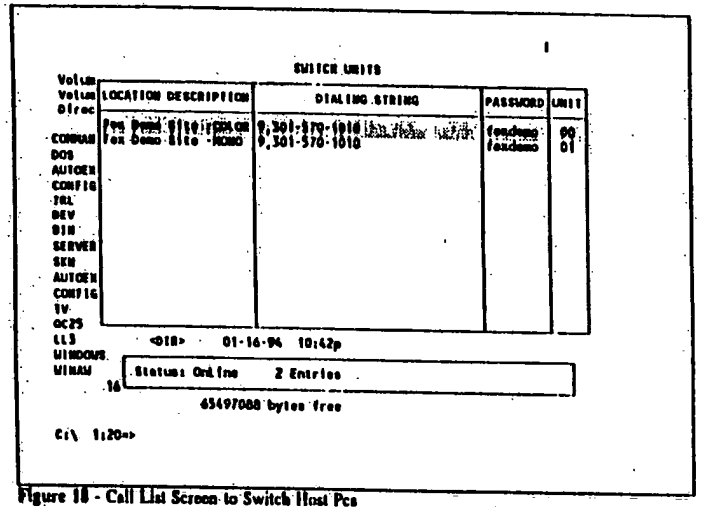

Figure 18 - Call List Screen to Switch Host Pcs

new KEY-VIEW unit is incorrect, the LOCAL PC will remain connected to the HOST site, but will not be connected to a KEY-VIEW unit as more fully described in section 3.3.0 above. Actions that may be taken in this situation are also discussed in section 3.3.0.

3.4.5 Unit Maintenance

This menu option permits changing the KEY-VIEW unit's password to a new password, updating the "Session Lock-out Limit", or updating the KEY-VIEW "Unit Lock-out Limit". When this menu option is selected, a menu permitting changes to the unit's password or lock-out limits appears as shown in the upper left-hand box on Figure 19. The Up Arrow or Down Arrow keys may be used to select the option to be changed, then press the Enter key to modify the option. As shown in Figure 19, the "Change Unit Password" option was selected causing the "Enter New

Password" window to pop up to allow the KEY-VIEW unit's password to be changed. If the Esc key is pressed while the Unit Maintenance menu is active, processing returns to the Connections Options menu.

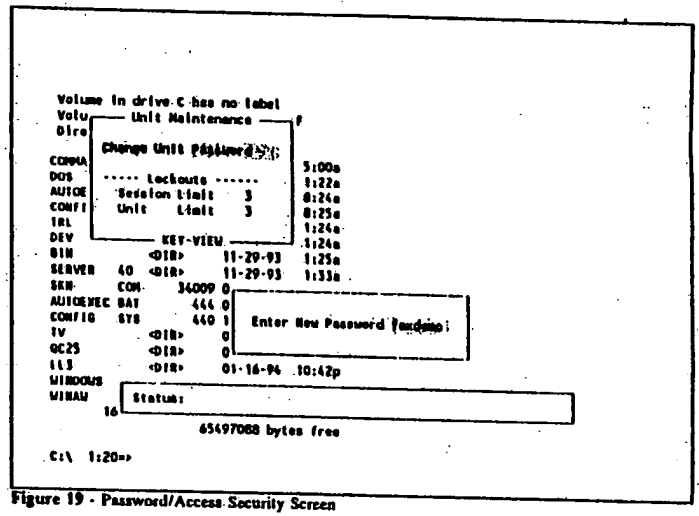

Figure 19 - Password/Access Security Screen

When a KEY-VIEW unit's password is changed, the call list entry for the applicable KEY-VIEW unit is automatically updated to reflect the new password. Care must be taken to inform any other authorized users of the unit's new password. Also, it is important to update the call list on any other LOCAL PC's that may be used to access the KEY-VIEW unit with the new password. The user is given the option to enter a new password of up to eight digits in length. Password change processing may be aborted by pressing the Esc key. When the Esc key is pressed, processing returns to the Unit Maintenance menu. Otherwise, after a new password is entered, the KEY-VIEW unit is immediately updated for the new password

and the applicable call list entry for the unit is automatically updated to reflect the new password.

The remaining Unit Maintenance menu options permit setting KEY-VIEW unit access security features that help preclude unauthorized access to a KEY-VIEW unit, as further illustrated in Figure 19. The "Session Limit" option permits setting the number of attempts during a session that a user is given to enter a valid password before being locked-out of this KEY-VIEW unit for the current session. An entry of "0" indicates that a user may be given an unlimited number of attempts to enter a valid password to access the KEY-VIEW unit. For purposes of lock-out processing, a session refers to the period of time between when a remote user first connects to a HOST site until the time the remote user terminates the phone connection to that site.

Once the "Session Limit" has been updated, the user may also update the "Unit Limit". The "Unit Limit" refers to the number of consecutive sessions that may occur where a user fails to specify a correct password to access a KEY-VIEW unit before the user is electronically locked-out of that KEY-VIEW unit. If the number of consecutive session lock-outs equals the limit specified, the KEY-VIEW unit will be electronically locked, until someone at the HOST site presses the "ACTION" button on the front of the locked out KEY-VIEW unit. In this case, the KEY-VIEW System could place an alert call to a pager using the pager dialing string setup, as discussed in section 2.4.0, so that someone will be notified of the possible intruder and unlock the unit in a timely manner. When a unit lock-out occurs that cannot be explained, it is strongly suggested that the phone number used to access the site be changed to a new phone number to help preclude any further unauthorized access attempts.

When a session at a HOST site ends (i.e. the connection is terminated), each KEY-VIEW unit automatically checks it's session lock-out counter. If the counter is not zero and less than the session lock-out limit, the counter is reset to zero and the unit lock-out count is increased by one. If the unit count then equals the limit, the KEY-VIEW unit is then electronically

locked, as previously discussed. This approach was taken to prevent someone from trying to guess the password by automatically terminating access to a KEY-VIEW unit immediately after the first access attempt fails or before the session lock-out limit is reached, so as to prevent a unit lock-out from ever happening.

When a user successfully accesses a KEY-VIEW unit and previous unauthorized access attempts have occurred, a warning message is displayed which includes the status of the unit lock-out counter. The authorized user is thus made aware that someone may be attempting to improperly access the unit. The unit lock-out counter is then reset to zero.

Once a KEY-VIEW unit is electronically locked, any user attempting to access that unit will be given a message in the KEY-VIEW Status box stating "Unit Is Locked Out" due to a possible intruder. In this case, any further access to the unit will be denied, even if a valid password is entered, until the "ACTION" button on the front of the KEY-VIEW unit is pressed. While electronically locked, the KEY-VIEW unit emits a periodic audible alarm sound and the "Keyboard Remote" indicator light on the front of the unit will blink ON and OFF until the "ACTION" button located on the front panel of the KEY-VIEW unit is pressed.

Each time a connection to a HOST site is terminated, each unit on the daisy-chain that has been electronically locked will cause a pager alert call to occur to the pager number specified during KVMODEM.EXE start up processing for KEYVIEW unit ID 00, as discussed in section 2.4.0. In this case the unit ID of the KEY-VIEW unit that has been locked will be automatically added to the end of the user specified pager alert code delivered.

A unit lock-out limit can be set to any number between "0" and "99". An entry of "0" indicates that the KEY-VIEW unit will not be electronically locked. The default setting for the session and unit lock-outs are 0. It is suggested that these default settings be changed to 3 or more for both the session and unit lock-out limits. Using a value of less than 3 may cause a

authorized user to be locked-out of a unit too quickly in cases when excessive line noise causes a password to be garbled and rejected by the HOST unit.

Both the session lock-out and unit lock-out features are security measures designed to prevent unauthorized intruders from guessing a password to a KEY-VIEW unit by limiting the number of guesses that can be made and bringing any unauthorized access attempts to the attention of authorized users. If lock-out capabilities are not desired, then simply set both the session and unit lock-out limits to "0".

Once the "Session Lockout Limit and the Unit Lockout Limit" have been set to desired values, press the Esc key to save the settings and return to the Connection Options menu.

Important: *Whenever a KEY-VIEW unit is switched "OFF" or AC power is lost, the counters containing the number of unauthorized session and unit access attempts are reset to zero when the KEY-VIEW unit is switched back "ON" or AC power is restored. Accordingly, in the rare case where there have been unauthorized access attempts and power is lost to a KEY-VIEW unit, a remote user accessing the KEY-VIEW unit after power is restored would not be advised of unauthorized access attempts, since the unauthorized access attempts counters would have been cleared.*

When setting the lock-out limits, the currently active lock-out limits will be initially displayed automatically. In cases where a lock-out limit is set, remote users will not be locked out until the limit is reached. For example, if the "Session Lock-out Limit" is 3, a remote user will not be locked from the unit for the session until the third consecutive access failed attempt. When a user is locked out during a session, a red box appears on the screen for about 5 seconds indicating "Security Breach - KEYVIEW Unit has been Locked - No More Accesses Possible". After the security breach message is displayed, processing automatically returns back to the KEY-VIEW Main Menu and the message "Session Locked Out" appears in the Status box.

In cases where security breaches are occurring, consideration should be given to requesting that the phone company change the phone number used to access the HOST site.

3.4.6 Print Host Screen

When selected, this Connection Option prints the current contents of the HOST PC's video display monitor to the LOCAL PC's default printer port or data file, in accordance with the Printer Setup options discussed in section 3.2.3. When a screen is printed, only the background HOST PC screen data is printed (i.e. the KEY-VIEW pop up menu is not printed). This screen printing feature gives KEY-VIEW users the ability to save HOST PC screen data as an audit trail. Maintenance contractors may find this feature particularly useful to save screen information to support client billings.

In rare cases, it is possible that the LOCAL PC may appear to lockup during printing. Normally, after about 30 seconds, a DOS message will appear indicating that the printer was not ready. At that point normal processing can be restored by either aborting printing or fixing the printer. Also, it will normally be necessary to refresh the screen by pressing the Right Shift key twice, rapidly, before trying to print the screen again.

Screens that are saved to a file instead of sent directly to a printer are saved in a standard text format. Such files can be subsequently viewed using any text file editor software program or printed to the default printer port using the DOS command "TYPE <file name> > PRN", where <file name> would be replaced with the printer file name specified in the Printer Setup menu (see section 3.2.3).

After the Host PC's screen data is printed, KEY-VIEW Main Menu processing ends and LOCAL PC processing automatically returns to the HOST Control mode.

3.4.7 File Transfer

This menu option permits file transfers to occur from the LOCAL PC to the HOST PC or vice-versa. File transfers from one directory location on a LOCAL PC to another directory location on the LOCAL PC can be accomplished by shelling out to DOS, as previously described under section 3.4.2. File transfers from one directory location on a HOST PC to another directory location on the same HOST PC may be accomplished by selecting the "Exit to HOST" option from the main KEY-VIEW Main menu. Then, use the LOCAL PC keyboard (that has been redirected to control the HOST PC keyboard) to complete the transfer using normal DOS COPY commands.

The file transfer feature of KEY-VIEW is a very useful procedure. For example, the procedure could be used to load NETWARE software patches to a file server from a remote location during non-business hours. In this case, a file server could be shut-down using the KEY-VIEW System from the remote location, the software upgrades could then be transferred to the DOS partition on the file server, and the file server re-started from the remote location using the newly installed software.

In order to complete a file transfer between a LOCAL PC and a HOST PC the KEY-VIEW unit must have been properly connected to one of the HOST PC's serial ports, as more fully described in section 2.1.0. Also, as discussed in section 2.4.0, a program called KVFILE.EXE must be accessible on a disk drive on the HOST PC. When necessary, KVFILE.EXE processing is initiated by a LOCAL PC to setup the necessary file transfer protocol and HOST PC serial port interface needed to transfer files between a HOST and LOCAL PC.

The first step in making a file transfer is to invoke the KVFILE.EXE

program on the HOST PC from a LOCAL PC. When KVFILE.EXE processing is initiated, the program checks the linkage between the HOST PC's serial port and the "SERIAL" receptacle on the back of the KEY-VIEW unit. If this serial connection cannot be made, either the message "<< COM PORT HAS NOT BEEN SPECIFIED >>" or "<< KEY-VIEW NOT FOUND >>" is displayed on the HOST PC. Refer to section 2.4.0, for a further description of these error messages and suggested corrective actions to be taken. If either of these messages appear, file transfer processing will not be possible until the serial linkage is restored and tested, as described in sections 2.4.0 and 2.1.0.

If no problems are detected when the KVFILE.EXE program is invoked, a box will be displayed on top left side of the HOST PC's screen indicating "KEY-VIEW - READY - FILE TRANSFER", as shown on Figure 20. The remainder of the screen illustrated on Figure 20 does not appear until a file transfer is initiated. File transfer processing on the HOST PC may be aborted at any time by pressing the Esc key on the LOCAL PC while the LOCAL PC is in control of the HOST PC's keyboard.

The next steps in the file transfer process are to press the **Left Shift** key three times on the LOCAL PC to pop up the KEY-VIEW Main Menu, select the "Connection Options" menu item, and then select the "File Transfer" menu option. When this menu option is selected, a menu containing two options appears, as shown in Figure 21. The first option permits file transfers to occur from the LOCAL PC to the HOST PC. The second option permits file transfers to occur from the HOST PC to the LOCAL PC. File transfer processing may be aborted by pressing the Esc key. If processing is aborted, KVFILE.EXE processing on the HOST PC should also be aborted after returning to the HOST PC by pressing the Esc key again on the LOCAL PC.

The **Up Arrow** and **Down Arrow** keys are used to toggle between the two file transfer options. The **Enter** key is used to select an option. Once selected, KEY-VIEW requests the entry of the file specifications defining the directory locations and file(s) to be copied, as shown in Figure 22.

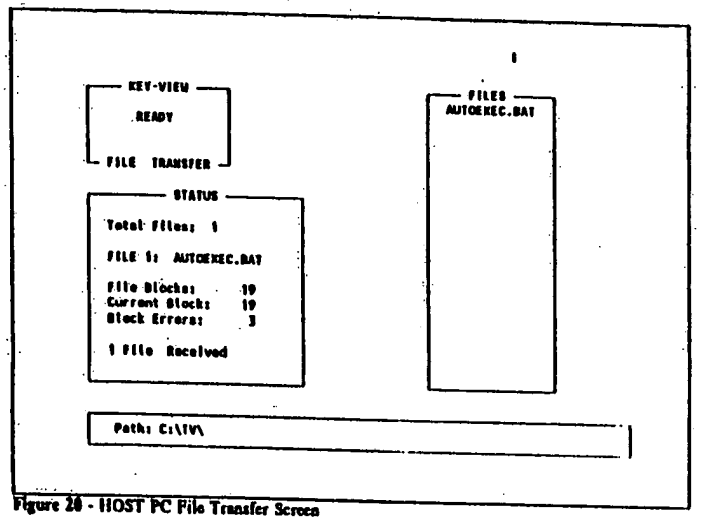

Figure 20 - HOST PC File Transfer Screen

When entering the specifications for the file(s) to be transferred, the drive and directory must be entered. The file name must also be entered, as appropriate, depending on the direction of the file transfer following conventions used for a normal DOS COPY command, including the use of the wild card "*" command. For example a source file could be specified as C:\NETWARE*.EXE, C:\VREPAIR.COM, or C:\NETWARE\VREPAIR.COM. Use the Up Arrow and Down Arrow keys to toggle between the LOCAL PC and HOST PC file specifications, press the Enter key to enter or modify the file specification entry, then press the Esc key to accept the specification entered. The destination directory where files are to be copied should always end with a back-slash "\" (e.g. C:\TV\ ).

After the LOCAL PC and HOST PC file transfer specifications have been entered, use the Down Arrow key to highlight the "Start File Transfer"

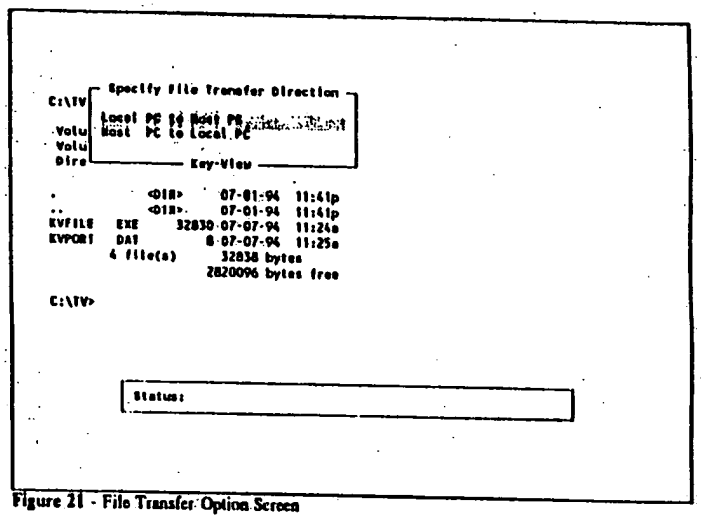

Figure 21 - File Transfer Option Screen

option and press the Enter key to begin the transfer process. At this point KEY-VIEW verifies that the KVFILE.EXE program has been activated on the HOST PC. If KVFILE.EXE has not been activated, the message "Could not Connect to Host" is displayed and processing returns to the Connection Options Menu. In this case, activate the KVFILE.EXE processing as described at the beginning of this section before re-attempting a file transfer. If the KVFILE.EXE program has been properly activated, the file specifications are validated to make sure the specified drives, directories, and source files exist. If they do not exist, an appropriate error message is displayed in the Status box and processing returns to the File Transfer Specifications window to permit the file specifications to be changed or the Esc key to be pressed to abort file specification processing.

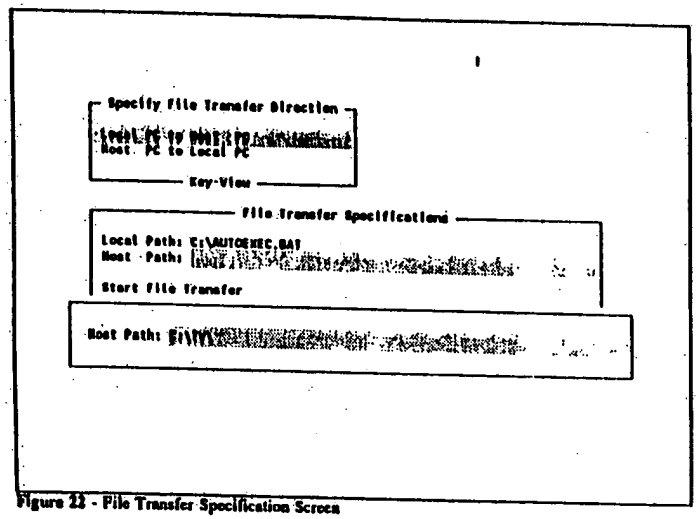

Figure 22 - File Transfer Specification Screen

While files are being transferred, processing may be aborted by pressing the Esc key. During the file transfer process, the name of each file being transferred is displayed along with the progress of the transfer, as shown in Figure 23. The "Errors" counter displayed reflects the number of file data blocks that were re-transmitted due to line noise. The status of each file transferred is also displayed on the HOST PC's screen, as shown on Figure 20, so that any personnel present at the HOST site can monitor the file transfer process.

After the requested files have been transferred, the message "File Transfer Complete" appears in the Status box. When the Esc key is pressed, processing returns to the File Transfer menu (see Figure 21). After all file transfers has been completed, press the Esc key to exit the KEY-VIEW pop up menus and return to the HOST PC's screen. Then, press the Esc key again to exit KVFILE.EXE file transfer processing on the HOST PC.

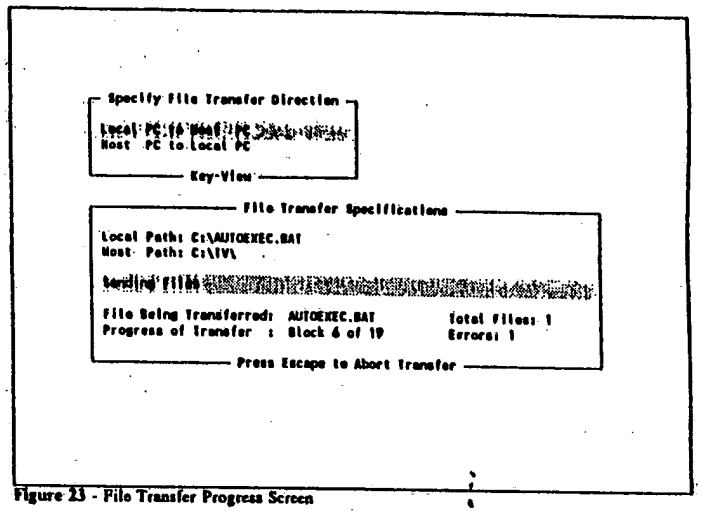

Figure 23 - File Transfer Progress Screen

3.4.8 Terminate Call

When this menu option is selected, the terminate call request must be confirmed by entering "Y" in response to the question "ARE YOU SURE? (Y/N)" (see Figure 24). If "N" or the Esc key is pressed in response to the question, call termination processing is aborted and processing returns to the Connections Options menu. If "Y" is entered, the connection between the LOCAL PC and the KEY-VIEW unit is terminated and processing returns to the KEY-VIEW Main Menu.

When a connection is terminated, the carrier detect signal on the HOST modem is dropped causing all units on the daisy-chain at a HOST site to reset automatically. After KEY-VIEW unit ID 00 resets, it automatically resets the modem connected to the unit. During this reset process the carrier detect signal is briefly turned ON then OFF. This action causes all

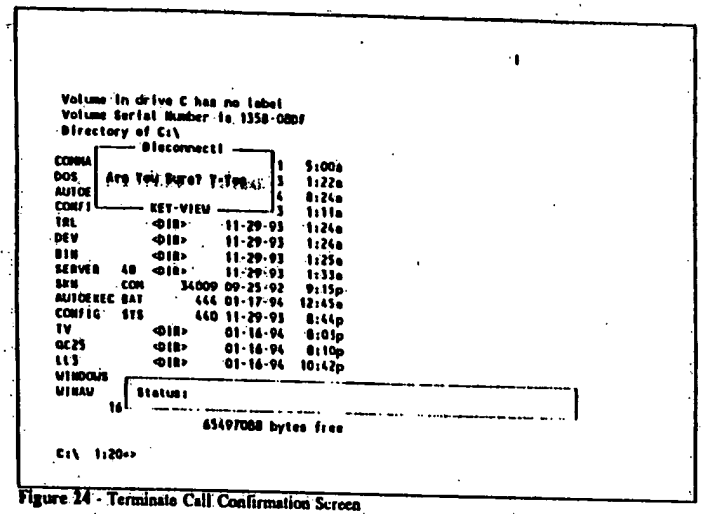

Figure 24 - Terminate Call Confirmation Screen

of the non-00 units on the daisy-chain to reset again. On this basis, it is normal for any non-00 units on a daisy-chain to reset twice after an access session has ended.

The process of resetting each KEY-VIEW unit when a connection is terminated or a carrier is lost is a critical, unique feature of the KEY-VIEW System. Unlike typical PC applications that may lock up a modem, requiring someone to go on-site to reboot the PC and/or modem, this automatic reset process ensures that each KEY-VIEW unit is ready for the next call.

A secondary measure is also taken to prevent each KEY-VIEW unit from locking up in cases where a telephone connection is not properly terminated (i.e. dropped) when a session ends. This situation could occur due to a malfunction of the commercial phone system where the LOCAL

PC side of the phone connection is terminated, but the HOST site modem still remains connected to the phone line. To automatically correct this situation, the KEY-VIEW software operating on a LOCAL PC periodically transmits an automatic "ping" signal to the HOST site during a session indicating the connection is still active. If this ping signal stops, the KEY-VIEW unit assumes the connection has been broken and each KEY-VIEW unit at the HOST site and the HOST site modem are reset forcing the phone line be cleared at the HOST site.

Each time a connection is terminated, KEY-VIEW unit ID 00 polls each of the other units on the daisy-chain to determine if any have been locked due to a security breach, as described in sections 3.4.5. If a unit has been locked and an alert phone number has been specified, as described in section 2.4.0 (using the KEY-VIEW KVMODEM.EXE program), an alert pager call will be placed for each KEY-VIEW unit that is locked.

3.4.9 Return to Main Menu

When this Connection Options menu item is selected or the Esc key is pressed while the Connection Options menu is active, processing returns to the KEY-VIEW Main Menu.

3.5.0 Exiting KEY-VIEW

The last menu option on the KEY-VIEW Main Menu permits exiting from the KEY-VIEW Main Menu, depending on the description of the menu option.

If the menu option is "Exit to HOST", it means a connection is active to a HOST PC, the KEY-VIEW software system will remain resident in memory, and processing will exit to a HOST Control mode (where the LOCAL PC will assume control of the HOST PC's keyboard and have full access to the HOST PC's video display output). After this menu option is selected, processing will return to the KEY-VIEW Main Menu, whenever the Left Shift key is pressed three times in rapid succession.

If the menu option is "Exit to DOS", it means a connection is active to a HOST site, the KEY-VIEW software will remain resident in memory and processing will temporarily shell-out to LOCAL PC DOS processing. Processing will return to the KEY-VIEW Main Menu, when the user enters "EXIT" at a DOS prompt then presses the Enter key.

If the menu option is "Exit System", it means no connection is active to a HOST site. When this menu option is selected, all KEY-VIEW LOCAL PC processing terminates and the user is returned to the LOCAL PC's DOS prompt.

4.0.0 VGA GRAPHIC DISPLAYS

This section only applies to KEY-VIEW units equipped with optional VGA processing capabilities. Users who do not have this option installed, or who are not using the VGA ports on the back of the KEY-VIEW unit should skip to section 5.0.0.

KEY-VIEW units equipped with the optional VGA interfaces have been designed to display either text or VGA graphics screens from a HOST PC on a LOCAL PC. After a KEY-VIEW unit has been trained to the specific display characteristics of a HOST PC, the KEY-VIEW unit can automatically determine whether a HOST PC is in a graphics or text screen mode and switch between these modes. In some cases, the LOCAL PC's screen may blank out when switching between video modes. If this occurs, follow the procedures discussed in section 6.4.0 to resume normal processing.

When a HOST PC is in a graphics mode, the data on the screen is composed of thousands of pixels (i.e. dots). The status of each pixel on a screen must be decoded and then transferred from the HOST PC to LOCAL PC and then re-coded and displayed on the LOCAL PC screen. This process takes substantially longer to accomplish than text mode transfers for which there is a maximum of approximately 2000 characters per screen.

When a Host PC is initially accessed or is switched to a graphics mode, a "snapshot" of the HOST PC's screen is taken and automatically transferred to the LOCAL PC's screen. The snapshot taken interprets each pixel on the screen as either black or white (i.e color and grey scaling is not presently supported). This process takes from between 30 seconds to 3 minutes to complete. During this time, the graphics screen is drawn from the top to the bottom of the screen similar to a fax transmission. Additional full screen snapshots occur whenever the user at the LOCAL PC taps the Right Shift key twice in rapid succession.

The additional time spent remotely displaying a graphics screen is usually only a minor inconvenience. Normally, a HOST PC is accessed via KEY-VIEW only when a graphics based application has locked up or failed. In such cases the remote user is only interested in the frozen snapshot of the current HOST PC screen display to determine what happened. Then, the remote user typically attempts to restart the application, which normally involves a few different data entry screens that will be frozen automatically by the application waiting for user input.

VGA Graphics applications normally display pixel data in various densities typically ranging from 640x480 pixels per screen to 1024x768 characters per screen. The pixel density for a HOST PC is governed by the type of video card and monitor being used, as well as the video settings for a particular application. Most PC graphics based applications, such as Microsoft's Windows, allow various pixel densities to be used depending on the capabilities of a given graphics card and monitor.

When a KEY-VIEW unit is trained during installation processing, the density is set to 640x480 pixels. This screen density was selected to avoid situations where higher density graphics screen transmissions could take more than 10 minutes without added benefit (i.e. the screen would not be significantly more readable if higher density video modes were transmitted to a LOCAL PC).

Any LOCAL PC used to access a HOST PC operating in a graphics mode must have a VGA compatible video display monitor. In addition, any application running on the HOST PC must be set to display graphics screens at a 640x480 screen resolution. Furthermore, it is suggested, but not typically necessary that the application be set to display video graphics data in a monochrome mode (i.e. color or grey scaling are not used). An example of procedures used to set a super VGA 1024x768 video card to a monochrome, 640x480 mode on a HOST PC running Microsoft Windows applications is discussed in section 4.1.0.

4.1.0 Microsoft Windows Graphics Interface

Microsoft Windows, like most typical PC graphics based applications or operating systems, permits setting a video card into a variety of video modes depending on the video card and monitor installed in a HOST PC. Typically, most HOST PCs running graphical applications have a Super VGA card and a color monitor capable of displaying pixel densities up to 1024x768. This section of the manual is intended to demonstrate the typical procedures used to setup Windows to best interface with the KEY-VIEW System. The sample procedure assumes a VGA or Super VGA card is installed in the HOST PC which will be set to a 640x480, monochrome mode using Windows 3.1. Also, remember in this example that any LOCAL PC used to access this HOST PC via KEY-VIEW in a graphics mode should also be capable of displaying 640x480 pixels.

The procedure used to setup the Windows video display to a monochrome mode is as follows:

(1) From the Program Manager Window select the MAIN icon

(2) From the MAIN window select the WINDOWS SETUP icon

(3) From the SETUP window select "Options"

(4) From the Options menu select "Change Systems Settings"

(5) Select the "Display Option Settings"

(6) Select the "VGA with Monochrome" Display Option

(7) Select OK to exit Change Systems Setting Menu

(8) At this point if the VGA with Monochrome driver was not previously loaded, Windows may ask that appropriate Install diskette with the driver be inserted

(9) Select option to "Restart Windows"

(10) When Windows is re-started the screen should then be in a monochrome mode

(11) Select the Control Panel icon from the Program Manager Window

(12) Select the Crayon icon from the Control Panel Window

(13) Select the "Color Scheme" window and set to "Monochrome"

(14) Click on the various parts of the example window (in the left center of the window) that have a high density of dots, then select a color pattern on the right side of the window that is either solid black, solid white, or has the fewest possible number of dots. This optional step helps speed up the windows graphics transfer by minimizing the number of pixel changes associated with intricate dot patterns.

(15) Save the Scheme

(16) Exit Windows - all suggested changes are now complete

5.0.0 UNIT STATUS INDICATORS

As shown on Figure 1, on page 12, there is a fuse status indicator light on the rear panel of the KEY-VIEW unit. When the KEY-VIEW unit is first turned ON, the left most two indicator lights on the front panel of the unit (see Figure 25,) should turn ON. If these indicator lights do not turn ON, it is likely that the 6.3 amp 250 volt slow blow fuse has blown and should be replaced by an identical new fuse. Slow blow fuses are normally available at most electronic stores or can be obtained from Fox Network Systems.

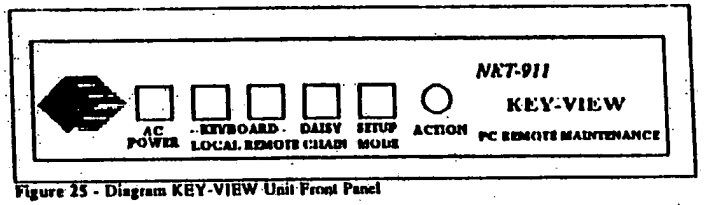

Figure 25 - Diagram KEY-VIEW Unit Front Panel

Figure 25 contains the front panel layout of the KEY-VIEW unit. The purposes for each indicator light on the front panel are as follows:

- The AC POWER light denotes the unit's ON/OFF switch is in the ON position and AC power is being received into the unit. When this light is flashing and the KEYBOARD LOCAL light is OFF, a remote user is in the process of cold-booting the HOST PC.

- The KEYBOARD LOCAL light indicates the keyboard attached to the HOST PC is available for use.

- The KEYBOARD REMOTE light indicates a remote user is accessing the HOST PC. If the light is blinking and a periodic beep sound occurs, it means the KEY-VIEW unit has been electronically

locked out due to a possible unauthorized intruder, as more fully discussed in section 3.4.5. If the light is ON, it means a remote user has taken control of the HOST PC's keyboard. (See section 6.1.0 for more information on coordinating remote and HOST user access to a HOST PC.)

- The DAISY CHAIN light blinks every half second indicating a remote user is currently connected to the site. If the DAISY CHAIN light is ON and not blinking, it means a remote user is currently accessing the KEY-VIEW unit. If no remote user is accessing the site, the light will be OFF.

- The SETUP MODE light flashes during the installation or re-configuration of the KEY-VIEW unit to indicate the unit is properly linked to the HOST PC or is in the process of training.

6.0.0 OTHER OPERATING PROCEDURES

6.1.0 Coordinating Simultaneous HOST PC Access

On occasion someone may be working at a HOST PC when a remote user attempts to access a HOST PC. Also, the user at a HOST PC site may wish to take control of the HOST PC keyboard away from an active remote user. Only one user can have control of the HOST PC's keyboard at any point in time. In cases of conflicts, the user at the HOST site has the final authority to determine who controls the HOST PC's keyboard, and control may be passed back and forth, as described in this section. Regardless of who has control of the HOST PC's keyboard, a remote user will have the ability to view the HOST PC's screen on their LOCAL PC after they have successfully logged into the HOST PC. LOCAL PC access to the HOST PC screen can be prevented at a HOST site by turning the KEY-VIEW unit's "ON/OFF switch OFF, then follow the procedures discussed in section 6.7.0.

When a LOCAL PC is initially linked to a HOST site, the "DAISY CHAIN" indicator light on all KEY-VIEW units at the HOST site will blink and will continue to blink as long as a LOCAL PC is linked to the HOST site. The HOST PC's keyboard is operable while the "DAISY CHAIN" light is blinking. When a specific KEY-VIEW unit at the HOST site is successfully accessed by a LOCAL PC using a valid password, the DAISY CHAIN light on that KEY-VIEW unit will stop blinking and remain ON. At this point the remote user specifies if they want full "Direct Access" to the unit or "View Only" access. If "Direct Access" is specified, the LOCAL PC assumes control of the HOST PC's keyboard and the KEYBOARD REMOTE light turns ON. Otherwise, the KEYBOARD REMOTE light remains OFF, the HOST PC's keyboard remains operable, and the LOCAL PC has no control over the HOST PC's keyboard. (NOTE: a blinking "KEYBOARD REMOTE" light and a

periodic "beep" sound indicate the KEY-VIEW unit has been locked due to a possible security breach, as more fully described in section 3.4.5)

When the "KEYBOARD REMOTE" light is ON, a user at the HOST PC could push the "ACTION" button on the front panel of the KEY-VIEW unit to assume keyboard control of the HOST PC. Once the "ACTION" button is pushed, a message pops up briefly on the LOCAL PC's screen stating "Keyboard Disabled" and a distinctive beep sound occurs. At this point the LOCAL PC no longer has control of the HOST PC's keyboard, but can continue to view the contents of the HOST PC's screen. Control can be returned to the LOCAL PC by pressing the "ACTION" button again in which case the message "Keyboard Active" will pop up briefly on the LOCAL PC's screen and the distinctive beep sound is repeated. By toggling the "ACTION" button as described, a user at the HOST site could chat with a user at a LOCAL PC via keyboard input, since both users have access to the HOST PC's screen and can simultaneously view what is being keyed.

If a remote user switches to a different KEY-VIEW unit on the Daisy-Chain or loses a connection to a KEY-VIEW unit, that KEY-VIEW unit will re-boot, the "KEYBOARD REMOTE" light will turn OFF, the "DAISY CHAIN" light will return to a blinking mode, and keyboard control will return to the HOST PC. These actions will also occur when a remote user terminates a connection to a HOST site, except in this case the "DAISY CHAIN" light turns OFF.

6.2.0 Hot Keys When Connected to a KEY-VIEW Unit

When a LOCAL PC is controlling a HOST PC keyboard, pressing the Left Shift key three times in rapid succession causes the KEY-VIEW Main Menu to pop up over the currently active HOST PC screen. This section discusses other hot keys that may be used when a LOCAL PC has assumed control of a HOST PC.

On occasion, the KEY-VIEW unit may misinterpret the HOST PC's video output signal causing "garbage" to appear on the LOCAL PC's screen. Such "garbage" can be eliminated by requesting the KEY-VIEW unit to refresh (i.e re-generate) the current screen. To request that the screen be refreshed, simply press the Right Shift key twice in rapid succession. This action will initially blank out the current screen and then re-generate the entire screen.

In rare cases, the KEY-VIEW unit's video translation table may become corrupted in memory. When this occurs, the screen may display a large number of block characters, "garbage" or simply go blank. In such cases, the translation table can be reloaded by pressing the Left Ctrl key three times in rapid succession. Then, wait for several seconds for the translation table to be reloaded into memory and the HOST PC's screen data to be re-generated.

6.3.0 LOCAL PC Keyboard Considerations

When a LOCAL PC is accessing a HOST PC, the use of the Caps Lock, Num Lock and Scroll Lock keys require special consideration. Software residing in the LOCAL PC keeps track of the status of these keys in both LOCAL and HOST keyboard control modes and restores the status of these keys whenever a LOCAL user switches between a LOCAL and HOST keyboard control mode. For example, if a LOCAL PC is presently in control of the HOST PC's keyboard and the user presses the Num Lock key ON, the Num Lock light on both the HOST PC's keyboard and the LOCAL PC's keyboard will turn ON. However, if the user hits the Left Shift key three times to pop up the KEY-VIEW Main Menu, the user may notice the Num Lock key light turns OFF because that was the prior state of the Num Lock key when LOCAL PC's keyboard was last active. In other words, the KEY-VIEW software automatically ensures that whatever was the last state of the keyboard is restored whenever the LOCAL PC's keyboard is switched between a HOST and LOCAL keyboard control mode. In some cases, this switching feature is important. For example the Num Lock key may need to be ON to properly operate a HOST PC

application, but must be OFF in order to select different menu options on the KEY-VIEW Main Menu.

Some applications have menu selection procedures where the menu light-bar does not scroll unless the Num Lock key on the keyboard is turned either OFF or ON. If this problem is experienced, try pressing the Num Lock key to a different setting, which should solve the scrolling problem.

In rare cases, the Shift key may be in a locked ON state. If this should occur, only special characters activated when the Shift key is pressed will appear, even though the Shift key is not being pressed. For example, when the "9" key is pressed ")" appears, when a "." character is pressed the ">" character appears, etc. To correct this problem simply press and release either Shift key once. A similar problem may also occur for the Ctrl key, where each key pressed is preceded by the "^" character (e.g. ^G, ^A, ^B, etc.). This problem can also be corrected by pressing and releasing the Ctrl key once.

When a HOST PC is re-booted by a KEY-VIEW unit, it is possible for the HOST PC to halt on an error such as "KEYBOARD ERROR - Press F1 to continue ..". This message occurs sometimes due to minor keyboard timing differences in the KEY-VIEW unit communicating with the HOST PC during the hardware initialization process. If this message should occur, simply press the F1 key. Halting in this manner is often desirable, because it gives the LOCAL PC enough time to synchronize with the HOST PC's screen while waiting for the F1 key press. In cases where a HOST PC re-boots where no LOCAL PC is connected to the KEY-VIEW unit, the boot process would not halt as a result of the KEY-VIEW connection to the HOST PC.

6.4.0 LOCAL PC Loss of HOST PC Video Screen

On occasion the LOCAL PC's video screen may go blank during a KEY-VIEW unit access session. Several actions may be taken to correct this problem, as follows:

(1) Hit the Left Shift key quickly three times to pop up the KEY-VIEW Main Menu. This action alone may solve the problem. If it does, simply exit from the Main Menu. If it does not resolve the problem, and the HOST PC is operating in a VGA mode; select the Connections Options menu, then select the "Set Video Mode" option. Next, select the "Mono Green" option, exit back to the Main Menu and then exit back to the HOST access mode.

(2) Hit the Left Ctrl key quickly three times and wait for about 10 seconds. This action will cause the entire video decode circuitry to reset and the video decode tables to be reloaded into the KEY-VIEW unit's memory.

(3) Hit the Left Shift key quickly three times to pop up the KEY-VIEW Main Menu. Select the Connections Options menu, then terminate the connection. Wait for about one minute for the KEY-VIEW unit to reset itself, then re-link to the KEY-VIEW unit.

6.5.0 Access to HOST PC's Hardware Configuration

It is normally desirable for a LOCAL PC to have access to the HOST PC's CMOS and other hardware configuration settings. Some PC's provide for Hot Keys or executable software to access such settings. In these cases, a LOCAL user would simply follow the normal KEY-VIEW procedures using the LOCAL PC's keyboard to change CMOS or other configuration settings for the HOST PC. However, a large number of PC's only permit access to CMOS and hardware configuration settings only for a few seconds immediately after the HOST PC is cold booted by pressing a designated key, which is typically the Delete key. Because of the time delay in transmitting video data from a KEY-VIEW unit to a LOCAL PC, there may not be enough time to depress this designated key at the correct time. To resolve this problem, a procedure could be employed whereby one of the CMOS setting could be set to an invalid setting. For example, the video setting could be set to monochrome even though a VGA monitor is connected to the HOST PC. Normally, an invalid setting will not

adversely affect the PC's operation, but will cause the HOST PC to always permit access to CMOS settings whenever the HOST PC is rebooted, as long as the invalid setting is not corrected and saved. Another possible approach that avoids setting CMOS to an invalid setting is to warm-boot the HOST PC by pressing the Ctrl, Alt and Delete keys together, then immediately tapping the Right Shift key twice to help speed up the screen refresh rate. Then, press the Delete key immediately when prompted on the screen.

6.6.0 Considerations When Daisy-Chaining Units

All KEY-VIEW units on a daisy-chain must be turned ON. If one of the units in the middle of the daisy-chain is defective or is turned OFF any units connected to the "DATA OUT" port of that unit through to the last unit in the daisy-chain will not be accessible by a LOCAL PC! The KEY-VIEW unit that is OFF or defective may be by-passed simply by unplugging the RJ-45 cables from the "DATA IN" and "DATA OUT" receptacles on the unit. Then, use an optional RJ-45 coupler (available from most electronic stores or Fox Network Systems) to join the two RJ-45 cables together, so that data will pass through the cable to the next unit on the daisy-chain. In cases where a KEY-VIEW unit is by-passed in this manner, the total length of the two cables joined together should be less than 250 feet.

6.7.0 Other Considerations

Whenever a KEY-VIEW unit is switched OFF or AC power is lost, the counter containing the number of unauthorized unit access attempts is reset to zero after the unit is switched back ON or AC power is restored. Accordingly, in the rare case where there have been unauthorized access attempts and power is lost to a KEY-VIEW unit, a remote user accessing the KEY-VIEW unit after power is restored would not be advised of any previous unauthorized access attempts.

When setting a password for a KEY-VIEW unit, remember that the password is case sensitive. For example, if the password set in the unit is "Tree", attempting to access the unit using "TREE", "tree", etc. will cause access to the unit to be denied!

When a KEY-VIEW unit is turned OFF, the video display monitor connected to the unit will go blank. This occurs because each KEY-VIEW unit processes then passes through the HOST PC's video signal to the video monitor. In cases where it is desired to leave the KEY-VIEW unit turned OFF, normal video processing can be restored to the HOST PC by disconnecting the video monitor's cable from the KEY-VIEW unit, unplugging the KEY-VIEW video cable connected to the HOST PC's video card, and connecting the video monitor's cable directly into the HOST PC's video card.

When a HOST PC is accessed, line noise on the telephone line may slow down data transmission rates or cause "garbage" to appear on the video screen. When line noise is present, such "garbage" sometimes appears in repetitive sets of random characters that display across then down the LOCAL PC's screen. In many cases, the line noise results from 1) someone picking up the same phone line or extension being used to access the HOST site, or 2) line cross-over noise at either the HOST or LOCAL site resulting from the phone system being improperly wired. If the problem occurs consistently, then it is suggested that dedicated phone lines be installed at both the HOST and LOCAL sites that are hooked directly to a telephone company jack.

In cases where line noise causes excessive "garbage" on the LOCAL PC's video screen, a normal video screen can usually be restored by pressing the Left Ctrl key three times in rapid succession. If this procedure doesn't work, the connection could be terminated to the HOST site and then re-connect to that HOST site. Such line noise will have no impact on the HOST PC's video display screen. With regard to keyboard input sent from a LOCAL PC to a HOST PC, extensive measures have been taken to stop any line noise from causing undesired input to occur to the HOST PC.

Older monochrome video interface cards and monitors have the capability to display each character with an underline under the character (e.g. A). This feature creates an entirely new character set for KEY-VIEW to decode. Sufficient memory does not exist within KEY-VIEW to decode this now obsolete character set. Since, very few applications use underlining, costly memory required for each KEY-VIEW unit to accommodate this rare situation was not added. Accordingly, if a KEY-VIEW unit is connected to a 9 pin, monochrome video display adapter card, the unit will not be capable of displaying any characters on the LOCAL PC that are underlined. Such characters will appear as solid blocks on a LOCAL PC. In cases where access to such underlined characters is necessary and the application cannot be changed to avoid the use of the underlined character set, it is suggested the HOST PC and KEY-VIEW unit be upgraded to include VGA capabilities, which generally solves the problem via color highlighting characters to indicate underlining.

KEY-VIEW does not presently support the XVGA standard on a HOST PC. In addition KEY-VIEW does not presently support the use of PC's with non-AT Compatible keyboards, except those PC's compatible with the new IBM Model 95 keyboard standard. In the case of the IBM Model 95 keyboard, support is presently only available for use of the Model 95 as a HOST PC. Support is not currently available for use of the Model 95 as a LOCAL PC. Refer to the README.TXT file for more recent information related to KEY-VIEW's compatibility with various hardware products.

7.0.0 FREQUENTLY ASKED QUESTIONS

QUESTION: Why doesn't the KEY-VIEW System allow HOST PC color or grey scale graphics screens to be viewed from a LOCAL PC?

ANSWER: KEY-VIEW is designed primarily as emergency monitoring system where access to screen data on a HOST PC must be reasonably timely.

In order to transmit color or grey scale graphics information from a HOST PC to a LOCAL PC each of the thousands of pixels comprising a screen must have a color and/or intensity attribute code. So instead of transmitting one bit of data for each pixel, several bits of data will be required, which will increase the delay in transmitting screen data to unacceptable levels. For example, it could take 20 minutes or more to transmit a full color graphics screen, as opposed to about 1 minute in monochrome. The actual transfer times will depend on the speed of the modem used and the quality of the phone line. When new technology supports greater telephone transfer speeds, KEY-VIEW will be enhanced to support color and grey scale graphics transfers.

QUESTION: Because of KEY-VIEW's powerful remote access capabilities, I am concerned about intruders gaining full remote control of our PC's or networks. What steps have been taken to prevent unauthorized access?

ANSWER: In addition to KEY-VIEW unit password protection discussed in section 3.4.5, and KEY-VIEW unit access security discussed in section 3.4.6, numerous other security features have been incorporated into the KEY-VIEW System.

First, a remote user must have a copy of the KEY-VIEW Installation diskette in order to attempt access to a KEY-VIEW unit. The KEY-VIEW System has been developed around unique, proprietary, communication protocols that will not allow a LOCAL PC access to a KEY-VIEW unit without the KEY-VIEW software programs. An intruder who did not have access to this software would stand virtually no chance of initiating a communications session with a HOST site.

Second, passwords sent by a LOCAL PC to a KEY-VIEW unit are encrypted using state of the art processes so that, even if someone were tapping into the phone line, they would stand virtually no chance of decoding the password being sent or even determining which data being transmitted was the password. For obvious security reasons, more specific information on how passwords are encrypted cannot be discussed in any further detail.

Third, any changes made to a password, lock out limits, etc. on a LOCAL PC are not visible to anyone at the HOST site (i.e. KEY-VIEW Main Menu and "Maintenance/Security" processing only appears on the LOCAL PC's screen).

Finally, even if someone had the means to access a KEY-VIEW unit, they would still need the phone number of the site.

QUESTION: What are the chances that the KEY-VIEW unit will accidently cut power to a HOST PC.

ANSWER: An extensive, complex series of codes must be transmitted by a LOCAL PC to a KEY-VIEW unit, and acknowledged by that unit, before the unit triggers a power cut to the HOST PC. On this basis it is highly unlikely for a software "glitch" or data transmission error to cause power to be cut to a HOST PC. From a hardware standpoint, a substantial amount of effort was directed to making the power cutting circuit fail safe.

When a remote user desires to cold-boot a HOST PC, the user must press the "Y" key to confirm the cold-boot process. Requiring the "Y" key to be pressed, as opposed to the Enter key, provides an extra measure of protection that a HOST PC is not inadvertently re-booted by a remote user.

QUESTION: One of the most frustrating problems in dealing with remote access systems is that they tend to lockup and can only be reactivated by going to the site and physically rebooting the system. When such lockups occur, these products are useless. What steps have been taken in the KEY-VIEW System to deal with system lockups.

ANSWER: The hardware circuits of a KEY-VIEW unit directly monitor the KEY-VIEW unit's modem carrier detect signal. When a call is placed via a LOCAL PC's modem to a KEY-VIEW unit, the carrier detect signal at the HOST site modem is automatically activated. If this signal is dropped for any reason, hardware circuits within each KEY-VIEW unit on the daisy-chain automatically reset themselves and unit ID 00 fully re-

initializes the HOST site modem. On this basis, it is highly unlikely for any software failure in the KEY-VIEW unit to preclude subsequent access to the unit.

Once accessed by the HOST site modem, the KEY-VIEW unit is periodically pinging the LOCAL PC to confirm the connection is still valid. If this pinging should cease for any reason (e.g. someone unplugs the RJ-45 data line, the phone line fails, etc.) an error message will appear on the LOCAL PC indicating the connection has been lost and each the KEY-VIEW unit on the daisy-chain will reset itself, as previously discussed. This pinging approach solves the problem where a phone line is not dropped at a HOST site after a LOCAL PC terminates the telephone connection.

8.0.0 ERROR MESSAGES & SUGGESTED ACTIONS

During a HOST site access session, several error messages may appear in the Status box on the LOCAL PC as follows:

Could Not Access Unit - This message means that KEY-VIEW unit ID specified in the LOCAL PC's call list (see section 3.2.1) does not appear to exist at the HOST site. In rare cases, a particular KEY-VIEW unit may lockup during initialization processing and not be accessible during an access section. Usually, this type of problem can be easily corrected by terminating the connection to the HOST site, which will cause each KEY-VIEW unit at the site to reset, then re-connecting to the HOST site.

If an incorrect KEY-VIEW unit ID was specified in the call list, change the unit ID to correct number (see section 3.2.1) while remaining connected to the HOST site, then use the "Switch Units" connection option (see section 3.4.4) to re-connect to the KEY-VIEW unit.

If the unit ID specified is known to be correct and repeated attempts to re-access the HOST site and KEY-VIEW unit fail then either (1) the KEY-VIEW unit is turned OFF or lost power; (2) the cable connection between the HOST site modem and KEY-VIEW units on the daisy-chain has failed or been disconnected; (3) the KEY-VIEW unit has failed; (4) there is excessive noise on the telephone line preventing a LOCAL PC from transmitting the correct unit ID or (5) another unit between the desired KEY-VIEW unit and the HOST site modem on the daisy-chain has failed or been turned OFF, thus breaking the daisy-chain connection to that KEY-VIEW unit.

No Video Signal Present - When this message appears the HOST PC screen is blank. This message means that no electrical signals are being received from the HOST PC video display adapter card. This situation will occur if (1) the cable between the KEY-VIEW unit and HOST PC's video

display adapter card has been disconnected, (2) the HOST PC's video adapter card has failed completely, or (3) the HOST PC has been turned OFF, failed or lost power.

Invalid Password --When this message appears an invalid password has been used in attempting to access the KEY-VIEW unit. Invalid password messages may appear in cases where excessive line noise interferes with the transmission of the password to the KEY-VIEW unit. If an incorrect password was specified in the call list, change the password (see section 3.2.1) while remaining connected to the HOST site, then use the "Switch Units" connection option (see section 3.4.4) to re-connect to the KEY-VIEW unit.

Remember that anyone with a valid password to a KEY-VIEW unit may change the password. In many cases, one user may have changed the password to a KEY-VIEW unit and not told other users about the change. In such cases the correct password must be obtained before access to the KEY-VIEW unit will be possible. If the password is lost or otherwise unobtainable, then the unit must be returned to Fox Network Systems to have the password reset.

If a password is believed to be both valid and current, terminate the HOST site modem connection and attempt to re-access the HOST site and KEY-VIEW unit. If this does not solve the problem, it is possible, but unlikely, that the memory where the password is stored in the unit has become corrupted or there is a lot of noise on the phone linkage between the HOST site and the LOCAL PC.

9.0.0 APPENDIX

APPENDIX	DESCRIPTION
A	KEY-VIEW Unit DIP Switch ID Settings

Appendix A

On the left rear side of the KEY-VIEW unit are DIP switches numbered 1 to 8. The left most 6 DIP switches numbered 1 to 6 determine the ID of the KEY-VIEW unit. Each KEY-VIEW unit on a daisy-chain must have a unique unit ID. Unit IDs need not be assigned sequentially, but the KEY-VIEW unit which is directly connected to the modem must be assigned Unit ID 00.

The table below shows the unit ID for each possible DIP switch setting. A switch value of "1" indicates a DIP switch is in the UP position (i.e closest to the top of the unit) and a value of "0" indicates a DIP switch is in the down position.

Unit ID Numbers for Dip Switch Settings

Unit ID	Switch# 123456	Unit ID	Switch# 123456	Unit ID	Switch# 123456	Unit ID	Switch# 123456
00	000000	16	000010	32	000001	48	000011
01	100000	17	100010	33	100001	49	100011
02	010000	18	010010	34	010001	50	010011
03	110000	19	110010	35	110001	51	110011
04	001000	20	001010	36	001001	52	001011
05	101000	21	101010	37	101001	53	101011
06	011000	22	011010	38	011001	54	011011
07	111000	23	111010	39	111001	55	111011
08	000100	24	000110	40	000101	56	000111
09	100100	25	100110	41	100101	57	100111
10	010100	26	010110	42	010101	58	010111
11	110100	27	110110	43	110101	59	110111
12	001100	28	001110	44	001101		
13	101100	29	101110	45	101101		
14	011100	30	011110	46	011101		
15	111100	31	111110	47	111101		

10.0.0 INDEX TO KEY-VIEW MANUAL

2400 BAUD (25)

A

AC MAIN INPUT (15)
AC OUT (15)
AC POWER (1), (2), (4), (5), (9), (11-13), (15), (16), (19), (24), (25), (57), (64), (79), (86)
AC TO PC (15)
ACCESS SECURITY (V), (61), (62), (90)
ACTION BUTTON (23)
ADAPTERS (5), (14), (19)
ALERT CALL (1), (27-29), (62), (63)
ANIMATED DEMONSTRATION (33), (34)
ANSWER ON RING (27)
APPENDIX (V), (17), (38), (95), (97)
ASCII (23)
AUTO ANSWER LIGHT (25)

B

BACKUP (1), (29), (36)
BATTERY (1)
BAUD (25), (27), (40-42)
BEEP (49), (79), (82)
BOOT (V), (3), (5), (12), (20), (26), (30), (31), (33), (53), (56), (57), (58), (82), (84), (86), (91)
BRIGHTNESS (54)

C

CABLE (5), (6), (9-16), (19), (24), (26), (29-31), (40), (41), (49), (86), (87), (93)
CALL LIST (V), (34), (36), (35), (37-39), (44-48), (59), (60), (59), (61), (62), (93), (94)
CAPS LOCK (83), (100)
CARRIER (25), (71), (72), (91)
CHAIN (4), (5), (16), (17), (24), (38), (63), (71-73), (80-82), (86), (91), (92), (93), (97)

CHAIN LIGHT (80), (81)
CHAT (82)
CMOS (2), (54), (85), (86)
COLD-BOOT (5), (31), (57), (91)
COLOR (8), (17), (37), (46), (52-56), (60), (75-78), (88), (89)
COLOR GRAPHICS (89)
COM911 (25), (27), (30), (41)
CONFIGURATION (4), (7), (20), (31), (32), (39), (41), (80), (85)
CONNECTION OPTIONS (V), (48), (49), (51-53), (56), (64), (67), (69), (73)
CONNECTION STATUS (34), (35), (52)
CONNECTOR (13-15), (24), (52)
COPYRIGHT (i), (21)
COULD NOT ACCESS UNIT (93)
CURSOR (40), (42), (54)

D

DAISY-CHAIN (4), (5), (16), (17), (24), (38), (63), (71-73), (86), (91), (92), (93), (97)
DATA IN (13), (16), (44), (76), (86)
DATA OUT (16), (18), (86)
DEFAULT PASSWORD (7), (38)
DIALING STRING (28), (37), (36), (37), (46), (59), (60), (62)
DIP SWITCH (V), (17), (18), (23), (38), (95), (97)
DIRECT ACCESS (51), (50), (81)
DIRECT CONNECT (10), (16), (17), (37), (40-42), (47)
DISPLAY MODE OPTIONS (V), (56)
DISTANCES (5)
DOS (9), (10), (12), (20), (23), (25-27), (30), (31), (33), (52), (53), (56), (55), (56), (58), (60), (61), (65), (66), (68), (72), (74)

E

ENCRYPTED (7), (47), (49), (90)
ERROR MESSAGES (67), (93)
EXIT SYSTEM (35), (74)

F

FILE TRANSFERS (7), (15), (56), (66), (67), (70)
FREQUENTLY ASKED QUESTIONS (89)
FRONT PANEL (V), (63), (79), (82)
FUSE (79)
FUSE STATUS INDICATOR LIGHT (79)

G

GARBAGE (22), (23), (83), (87)
GRAPHIC SNAPSHOT (55)
GRAPHICS MODE (51), (53), (55), (75-77)
GREY SCALE (89)

H

HAYES COMPATIBLE (16), (25), (28), (33), (42)
HAYES MODEM (40), (41)
HELP SCREEN (V), (39), (59)
HOST SYSTEM MENU (V), (46)
HOT KEYS (33), (82), (85)

I

IBM MODEL 95 (18), (23), (88)
INDEX (V), (99), (100)
INSTALLATION (iii), (6), (7), (9-12), (20), (25), (26), (32), (33), (41), (76), (80), (90)
INTENSITY (54), (89)
INTRUDER (28), (50), (62), (63), (80), (90)
INVALID PASSWORD (29), (49), (94)

K

KEYBOARD (1), (3), (4), (8), (9), (11-14), (28), (33), (43), (50), (56), (58), (59), (63), (66), (67), (73), (79-85), (87), (88)
KEYBOARD ACTIVE (82)
KEYBOARD DISABLED (82)
KEYBOARD ERROR - PRESS F1 TO CONTINUE (84)
KEYBOARD INPUT FROM KB (13)
KEYBOARD OUTPUT TO PC (13)
KEYVIEW.BAT (33-35)
KVFILE (ii), (25), (28-31), (66-70)
KVLINK (34)
KVMODEM (V), (26-27), (29), (31), (32), (63), (73)
KVTRAIN (ii), (12), (20), (22)
KVWAIT (25), (31)

L

LEFT SHIFT KEY (50), (55), (56), (67), (73), (82), (83), (85)
LICENSE (ii), (7), (33)

LICENSE FEES (7), (33)
LIGHT BAR (84)
LINE NOISE (42), (47), (48), (64), (70), (87), (94)
LINKAGE (26-30), (32-34), (42), (47), (48), (67), (94)
LOCAL LIGHT (79)
LOCATION DESCRIPTION (37), (36), (46), (60)
LOCK-OUT COUNTER (49), (50), (62), (63)
LOCKED (1), (2), (7), (28), (48), (49), (58), (62-65), (73), (76), (80), (82), (84)
LOCKED UP (2)
LOCKS (2)
LOCKUPS (91)

M

MAXIMUM DISTANCES (5)
MEMORY (2), (7), (19), (29), (33), (56), (73), (74), (83), (85), (88), (94)
MINI KEYBOARD (9)
MODEM SETUP (V), (7), (18), (17), (26-28), (34), (36), (40)
MONO (37), (46), (53), (55), (56), (60), (85)
MONOCHROME (1), (6), (8), (12), (14), (17), (20), (52-55), (76), (77), (78), (85), (88), (89)

N

NO VIDEO SIGNAL PRESENT (49), (93)
NON-VGA (9), (17), (20), (52), (53)
NON-VOLATILE MEMORY (19), (29)
NOTICES (I), (II)
NUM LOCK (83), (84)

O

ON/OFF SWITCH (10), (18), (79), (81)

P

PALMTOPS (34)
PASSWORD (V), (7), (8), (11), (29), (37), (38), (46-50), (60), (59), (60-64), (81), (87), (90), (94)
PIXEL (20), (23), (75-78), (89)
POWER LIGHT (79)
PRINT HOST SCREEN (53), (56), (65)
PRINTER EJECT (45), (51)
PROTOCOL (29), (66)
PS-2 (9), (14)

R

RE-BOOTED (84), (91)
RE-TRAIN (19)
README (III), (9), (25), (26), (33), (42), (88)
REAR PANEL (V), (12), (79)
RECEPTACLE (10), (13-16), (67)
REMOTE LIGHT (79), (81)
RESET (7), (8), (25), (40), (42), (47), (48), (50), (62-64), (71), (72), (73), (85), (86), (91-94)
RIGHT SHIFT KEY (55), (65), (76), (83), (86)
RJ-11 (5), (10), (19)

S

SCAN FACTOR (22)
SCAN STATUS (21)
SCROLL (46), (59), (83), (84)
SCROLL LOCK (83)
SECURITY (V), (3), (8), (11), (47), (48), (50), (61), (62), (64), (65), (73), (82), (90)
SECURITY BREACH (64), (65), (73), (82)
SEND TO FILE (43), (44)
SEND TO PRINT (44)
SENSITIVE (7), (11), (37), (87)
SERIAL (5), (7), (9), (10), (13), (15), (16), (26), (27), (29), (30), (40), (41), (47), (52), (58), (66), (67), (72)
SESSION (2), (5), (8), (23), (34), (35), (44), (49), (52), (60-65), (72), (73), (84), (90), (93)
SESSION LOCK-OUT (60), (62-64)
SET DISPLAY MODE (53), (52), (53), (55), (56)
SETUP STRING (7), (26)
SHIFT KEY (50), (55), (56), (65), (67), (73), (75), (82-86)
SIMULTANEOUS HOST PC ACCESS (81)
SNAPSHOT (55), (56), (75), (76)
SPEAKER LEVEL (27), (40), (42)
SPEAKER STATUS (27), (40), (42)
STATUS (V), (4), (21), (27), (34-37), (40), (42), (46-53), (56-58), (60), (61), (63), (65), (68-70), (72), (75), (79), (83), (93)
SWITCH BOX (11)
SWITCH HOST/LOCAL MODE (48), (55), (56)
SWITCH UNITS (48), (50), (53), (56), (59), (60), (59), (93), (94)
SWITCHER (1), (13), (15), (16)

T

TABLE OF CONTENTS (III)
TAMPERING (7), (8)
TECHNICAL SUPPORT (III), (19), (20)
TELEBOOT (2)
TERMINATE CALL (V), (53), (56), (59), (71), (72)
TEXT MODE (53-55), (75)
TRADEMARK (I)
TRAINING (V), (6), (18-21), (20), (21), (20-24), (80)
TRANSFER RATES (54)

U

UNAUTHORIZED ACCESS (7), (62-64), (86), (89)
UNIT FRONT PANEL (V), (79)
UNIT ID (V), (17), (24), (32), (38), (41), (47), (48), (63), (71), (73), (91), (93), (97)
UNIT IS LOCKED OUT (49), (63)
UNIT LOCK OUT (28), (49), (50), (60), (62-64)
UNIT MAINTENANCE (53), (56), (60-62)
UNIT REAR PANEL (V), (12)
UNIT STATUS INDICATORS (79)
USER.DAT (34), (39), (41)

V

VGA (1), (6), (8-10), (12-14), (17), (20), (21), (23), (52-55), (75), (76), (77), (85), (88)
VGA GRAPHICS (1), (20), (53), (55), (75), (76)
VGA IN (13), (14)
VGA OUT (14)
VIDEO CARD (5), (6), (11), (12), (19-23), (31), (52), (76), (77), (87)
VIDEO IN (13), (14)
VIDEO MODES (1), (75-77)
VIDEO OUT (14)
VIEW ONLY (76), (81)

W

WARM BOOT (58)
WARRANTY (I), (II), (10)
WINDOWS (II), (33), (41), (51-53), (56), (58), (60), (61), (72), (76), (77), (78)